

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-178164

(43)Date of publication of application : 27.06.2003

(51)Int.Cl.

G06F 17/60

G06F 12/14

G06F 15/00

H04L 9/08

(21)Application number : 2002-270625

(71)Applicant : FUJITSU LTD

(22)Date of filing : 06.04.1999

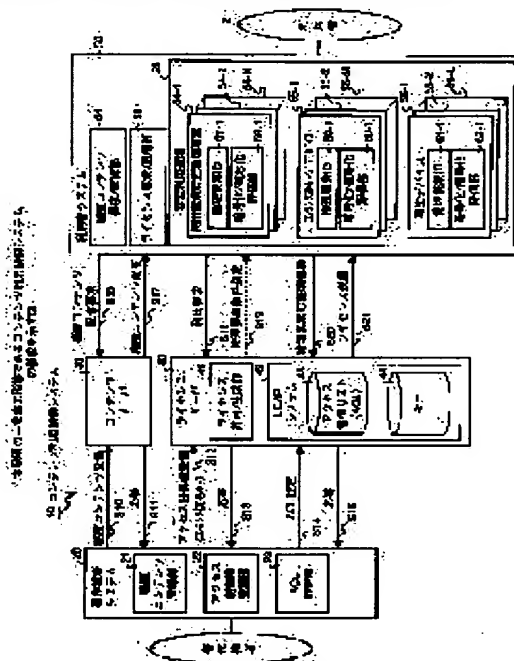
(72)Inventor : HATAKEYAMA TAKAHISA
YOSHIOKA MAKOTO
MIYAZAWA YUJI

(54) LICENSE MANAGING DEVICE, LICENSE MANAGING METHOD AND LICENSE MANAGING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide flexible contents utilization control and accurate prevention of fraudulent utilization of contents to an information provision authority.

SOLUTION: A copyright holder system 20, a contents server 30, a license server 40 and a user system 50 are provided. An ACL setting part 23 of the copyright holder system 20 sets a plurality of partial utilization permission conditions with respect to the contents as structurally represented utilization permission conditions ACL by a combination of logical sums and logical products on the basis of a user ID and IDs of a plurality of physical elements including a medium used in the user system 50, and stores them in an access control list 43. The license server 40 encrypts the access control list 43 and a decipher key Kc by combining the plurality of physical element IDs.



LEGAL STATUS

[Date of request for examination]

17.09.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

3749212

[Date of registration]

09.12.2005

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision of
rejection]

[Date of extinction of right]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The use authorization conditions of these contents are managed with the decode key which decodes the enciphered contents. It is license management equipment with which answers a contents use demand from a user, enciphers this decode key and use authorization conditions, and a user is provided as a license. A physical element path storage means by which the information on a physical element that a license would win popularity in order and would be passed by the time said decode key is used for decode of contents was memorized, License management equipment characterized by having a license generation means to encipher said decode key and use authorization conditions based on the information on the physical element memorized by said physical element path storage means, and to generate a license.

[Claim 2] Said license generation means is license management equipment according to claim 1 characterized by enciphering said decode key and use authorization conditions combining the proper identifier of two or more of said physical elements, and generating a license including the proper identifier of two or more physical elements which a license receives in order the information on the physical element memorized by said physical element path storage means, and are passed.

[Claim 3] Said license generation means is license management equipment according to claim 2 characterized by enciphering with the gestalt which can be decoded using a proper identifier from the license from which this each of physical element received the element conditions that each physical element could be forced, among the element conditions which constitute said use authorization conditions.

[Claim 4] It is license management equipment according to claim 2 or 3 which two or more physical elements the proper identifiers were remembered to be by said physical element path storage means are a record medium, a recording device, and a regenerative apparatus, and is characterized by enciphering said license generation means based on the proper identifier which said record medium, a recording device, and a regenerative apparatus have.

[Claim 5] Said license generation means is license management equipment according to claim 4 characterized by enciphering using the exclusive OR of the proper identifier of said record medium, and the proper identifier of a recording device after enciphering using the proper identifier of said regenerative apparatus.

[Claim 6] The use authorization conditions of these contents are managed with the decode key which decodes the enciphered contents. It is the license management method with which answers a contents use demand from a user, enciphers this decode key and use authorization conditions, and a user is provided as a license. The physical element path registration process of registering the information on a physical element that a license will win popularity in order and will be passed by the time said decode key is used for decode of contents, The license management method characterized by including the license generation process which enciphers said decode key and use authorization conditions based on the information on the physical element registered according to said physical element path registration process, and generates a license.

[Claim 7] Said license generation process is a license management method according to claim 6 characterized by enciphering said decode key and use authorization conditions combining the proper identifier of two or more of said physical elements, and generating a license including the proper identifier of two or more physical elements which a license receives in order the information on the physical element registered according to said physical element path registration process, and are passed.

[Claim 8] Said license generation process is a license management method according to claim 7 characterized by enciphering with the gestalt which can be decoded using a proper identifier from the license from which this each of physical element received the element conditions that each physical element could be forced, among the element conditions which constitute said use authorization conditions.

[Claim 9] It is the license management method according to claim 7 or 8 which two or more physical elements the proper identifiers were remembered to be according to said physical element path storage process are a record medium, a recording device, and a regenerative apparatus, and is characterized by enciphering said license generation process based on the proper identifier which said record medium, a recording device, and a regenerative apparatus have.

[Claim 10] Said license generation process is a license management method according to claim 9 characterized by enciphering using the exclusive OR of the proper identifier of said record medium, and the proper identifier of a recording device after enciphering using the proper identifier of said regenerative apparatus.

[Claim 11] The use authorization conditions of these contents are managed with the decode key which decodes the enciphered contents. It is the license manager with which answers a contents use demand from a user, enciphers

this decode key and use authorization conditions, and a user is provided as a license. The physical element path registration procedure of registering the information on a physical element that a license will win popularity in order and will be passed by the time said decode key is used for decode of contents, The license manager characterized by performing the license generation procedure which enciphers said decode key and use authorization conditions based on the information on the physical element registered by said physical element path registration procedure, and generates a license by computer.

[Claim 12] Said license generation procedure is a license manager according to claim 11 characterized by enciphering said decode key and use authorization conditions combining the proper identifier of two or more of said physical elements, and generating a license including the proper identifier of two or more physical elements which a license receives in order the information on the physical element registered by said physical element path registration procedure, and are passed.

[Claim 13] Said license generation procedure is a license manager according to claim 12 characterized by enciphering with the gestalt which can be decoded using a proper identifier from the license from which this each of physical element received the element conditions that each physical element could be forced, among the element conditions which constitute said use authorization conditions.

[Claim 14] It is the license manager according to claim 12 or 13 which two or more physical elements into which the proper identifier was registered by said physical element path registration procedure are a record medium, a recording device, and a regenerative apparatus, and is characterized by enciphering said license generation procedure based on the proper identifier which said record medium, a recording device, and a regenerative apparatus have.

[Claim 15] Said license generation procedure is a license manager according to claim 14 characterized by enciphering using the exclusive OR of the proper identifier of said record medium, and the proper identifier of a recording device after enciphering using the proper identifier of said regenerative apparatus.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention manages the use authorization conditions of contents with the decode key which decodes the enciphered contents, and it is related to the license management equipment, license management method, and license manager with which answer a contents use demand from a user, encipher a decode key and use authorization conditions, and a user is provided as a license.

[0002] A monetary role provides people with fair remuneration with the property as matter called the money. As for an object called money, it was indispensable requirements not a mere verbal agreement-share concept but for forgery [further / exist physically, can carry and / in addition to a publishing agency] to be difficult. It existed physically, and by being portable, it could check impartially by the users of the value, and fair money issue-origin was able to control the opportunity of the fair check by counterfeit difficulty. However, the day when now monetary forged difficulty will collapse by development of a technology in recent years is near. The new value check object replaced with money is needed. It is necessary to exist physically too first, and the object can be carried and needs to be difficult to forge. Furthermore, the object carries out the access control of the publishing agency.

[0003] In addition to the demand from this security strengthening side, the demand of implementation of a "superdistribution" is also increasing from the side face of diversification of the distribution of information, large-capacity-izing, and improvement in the speed. The environment which realized this "superdistribution" satisfies the following conditions. that (1) information user can obtain digital information for free mostly, that the conditions on which (2) information providers specified the conditions (accounting, alteration use conditions, etc.) to which use of that information is permitted, and the user has agreed can be forced, and (3) — in using this service, a required information user's add operation is "check of access condition" extent — it comes out. [namely,]

[0004] It is expectable that accuracy and the system which can be performed safely contribute the access control of such a superdistribution also to unfair correction of royalty collection, such as a charge of a license. the present system — a work — about — although a provider cannot gain profits unless it can sell a number, to be able to build a system so that it may cross to a copyright person's hand correctly is desired. Moreover, the remuneration corresponding to each one of service charges is wanted to be distributed impartially until it results [from an expert-artist] in the designer who offers creation as components.

[0005]

[Description of the Prior Art] When access to contents, such as a work, was conventionally controlled on a distributed-system environment, especially an open network, use of contents was controlled by storing contents in the server which can be accessed from the user of contents, and controlling access to this server. Here, contents are digital contents with the structure recordable on a single store medium as a set of a bit string, and a document text, an image, an animation, program software, etc. are included.

[0006] For example, drawing 17 is drawing showing the conventional access-control model. In drawing 17, contents 204 are enabling contents actuation from a user 205 through the access-control function 203. Moreover, for example, the copyright person 200 was taken care of by the access-control function 203 in contents 204, it is only registering with a server and the access-control actuation to the access-control function 203 was made by persons other than copyright person 200, for example, the manager who manages this server.

[0007] That is, it is managed by the server employment person system 211 in which management employment is done by the manager 201, and the server employment person system 211 performs a copyright person and a user registration to the server system 212, and the server system 212 which holds contents as shown in drawing 18 performs directory generation for it, and also performs permitting the access control by the copyright person further. The copyright person system 210 makes the contents of a copyright person's work save in the server system 212, and sets up access-control conditions (ACL) to the server system 212. In this case, a copyright person has to get authorization of an access control to the server system 212. On the other hand, the user system 213 acquires the contents saved in the server system 212, when performing a contents Request to Send to the server system 212 and satisfying ACL on the occasion of use of contents.

[0008] However, if all authority is granted to the user of contents and a user changes by migration or the copy (duplicate), to the contents of migration or a copy place, the authority of the copyright person of a basis will not be committed at all. Moreover, between the server manager who saves a contents object, and the copyright person, the state of access consent compulsion to an object is not clear, either, for example, a copyright person does not refuse and have a server manager, and to be able to change an access privilege was made into the natural thing.

[0009] On the other hand, without the distributed-system environment's having been promoted by low-pricing of a storage in recent years etc., and network traffic concentrating by it, the cache of the contents can be carried out to two or more servers, it can distribute now, and access to a contents object could be performed at the high speed. Therefore, although the access-control model as shown in drawing 17 should just build the firm access-control function only to the entry to the contents actuation by the user 205, it needed to perform all the directions-access control or security protection under the distributed-system environment mentioned above.

[0010] Then, the access-control model as shown in drawing 19 was able to be considered. The copyright person 200 is separated into the copyright person protected area which is a field which can be protected, the open field which receives the attack from all the outside, and protection of an alteration of hard/software and the secrecy protected area to which digital data duplicate prevention processing is performed by the conventional security technique in this access-control model. A secrecy protected area is protected by the omnidirection access-control function 221, and contents 222 are saved in this access-control function 221.

[0011] The copyright person 200 is also enabling access-control actuation to the access-control function 221 with registration of contents 222 to these contents. A user 205 will acquire contents 222 from an open field through the access-control function 221. In addition, the field protection interface 220 is an interface which performs protection between a copyright person protected area and an open field.

[0012] Somatization of the access-control model under the distributed-system environment shown in this drawing 19 is indicated by the U.S. Pat. No. 5339403 number official report, and the technique of checking a user's device in JP,9-134311,A, a U.S. Pat. No. 5392351 number official report, a U.S. Pat. No. 5555304 number official report, and a U.S. Pat. No. 5796824 number official report, and preventing unjust use of contents in them is indicated. Hereafter, the conventional contents use control system is explained with reference to these official reports.

[0013] Drawing 20 is drawing showing the contents distribution model of the conventional contents use control system. In drawing 20, it is equivalent to the secrecy protected area indicated to be a decode protected area and a playback protected area to drawing 18, a decode protected area is a field of protection of an alteration of hard/software, and duplicate prevention protection of output data, and a playback protected area is a field of duplicate prevention of digital decode data. The use environmental specification physical element (PCSUE) 235-1 - 235-N are physical elements which specify the use environment of contents, and, specifically, are CPU, a peripheral device, a removable storage, an IC card, etc.

[0014] In a decode protected area, the contents 234 which are the duplicates of the contents 233 enciphered by the copyright person 200, and exist in the server of an open field are decoded based on the certificate 236-1 of the physical element ID corresponding to PCSUE 235-1 - 235-N - 236-N, and these compounded contents are used for a user through a playback protected area. Therefore, contents are enciphered by the key corresponding to a physical element ID (contents 233), and in order to decode the contents 234 corresponding to these contents 233, each physical element ID or the secret key corresponding to it is needed.

[0015] A license has the contents cache possible mold model acquired to another timing by saving the contents enciphered as the license coincidence model which distributes the license used for a contents distribution model here in order to decode the enciphered contents to the enciphered contents and coincidence into the cache of a server. Drawing 21 is drawing showing this contents cache possible mold model.

[0016] In drawing 21, first, it is a copyright person protected area, and an author 200 generates contents and enciphers these contents, after that, he reproduces and a cache is done to the server of an open field etc. On the other hand, the certificate 241-1 which enciphered the physical element ID of PCSUE 235-1 - 235-N - 241-N It is outputted to a copyright person protected area in the condition of having been enciphered, and a secret key Kp is taken out from the user physics object class corresponding to PCSUE 235-1 - 235-N. This secret key Kp, and a certificate 241-1 - 241-N to a physical element ID 243-1 - 243-N are decoded, and by this physical element ID 243-1 - 243-N, the contents decode key Kc is enciphered and it outputs to a security field.

[0017] In a security field, the enciphered contents decode key Kc is decoded by the physical element ID 242-1 - 242-N, and the contents decode key Kc is obtained. The enciphered contents 234 which are acquired from an open field using this contents decode key Kc are decoded, and a user 205 is made to use as contents 244.

[0018] Drawing 22 is the block diagram showing the outline configuration of the contents use control system corresponding to the contents cache possible mold model shown in drawing 21. In drawing 22, the copyright person system 250 exists in a copyright person protected area, the contents server 251 exists in an open field, and a license server 252 and the user system 253 exist in a secrecy protected area. The copyright person system 250 enciphers the created contents, and saves these enciphered secrecy contents at the contents server 251.

[0019] Moreover, the contents decode key Kc is transmitted to a license server 252, and the transfer of the right of an access control is performed to a license server 252. Furthermore, an access control list (ACL) setup is performed. When the use demand which shows that contents are used is transmitted to a license server 252 and the certification group of a physical element ID is not attached at this time, by the physical element criteria specification of a license server 252, the user system 253 acquires the certification group of a physical element ID, and sends it out to a license server 252.

[0020] A license server 252 acquires the secret key Kp of a user's physical object class, as shown in drawing 21, and the contents decode key Kc enciphered with the physical element ID which decoded and decoded the physical element ID certification group is sent out to the user system 253 as license L. If the physical element ID of the user system 253 is in agreement, decode is performed by this and secrecy contents can be decoded by it using this decoded contents decode key Kc.

[0021] In addition, since secret contents are saved at the contents server 251, the user system 253 needs to perform a secret contents distribution request to the contents server 251 separately, and needs to receive distribution of secret contents from the contents server 251.

[0022] On the other hand, drawing 23 shows the outline configuration block Fig. of the contents use control system which realizes a contents coincidence distribution mold model. In drawing 23, the contents server 251 will not exist but it will be sent to the user system 253 at license transmission and coincidence. Since secret contents are beforehand carried to the server near the user system 253 in time when acquiring secret contents through the contents server 251 as shown in drawing 22, the user system 253 should just carry out a use demand, when contents are required.

[0023] Moreover, suitable selection of the distribution channel of contents is attained as compared with a contents coincidence distribution mold model, and compaction of the response time can be expected on the occasion of contents acquisition for a user. Moreover, it is possible to distribute contents beforehand with the cache by the ROM medium base, broadcast, and the Proxy server etc. apart from offer of a license in a contents cache possible mold model, and there are many advantages.

[0024]

[Problem(s) to be Solved by the Invention] However, although secrecy contents can be decoded fundamentally and these contents can be used in the conventional contents use control system mentioned above if it is equipment which is in agreement with a user system at the physical element ID of a proper Since this physical element ID is generating the license (use authorization conditions) For example, the conditions which restrict the count of read-out of the contents determined with a copyright person's intention could not be added, a time limit could not be prepared, accounting conditions could not be set up, but there was a trouble that flexible contents use control could not be performed.

[0025] Moreover, it did not restrict having always simple composition, but when it was a device with a complicated configuration, a use environmental specification physical element may have inaccurate specific device or specific components of the device, and even if it generated use authorization conditions with the use environmental specification physical element which is the device of an only big configuration, in such a case, there was a trouble overlooking injustice and that security fell.

[0026] while, as for this invention, an information offer authority person including those who were made in view of the above and permitted by information implementers, such as a copyright person, can perform contents use control flexibly — unjust use of contents — precision — it aims at offering the license management equipment which can be prevented highly, a license management method, and a license manager.

[0027]

[Means for Solving the Problem] In order to solve the technical problem mentioned above and to attain the purpose, this invention The use authorization conditions of these contents are managed with the decode key which decodes the enciphered contents. It is license management equipment with which answers a contents use demand from a user, enciphers this decode key and use authorization conditions, and a user is provided as a license. A physical element path storage means by which the information on a physical element that a license would win popularity in order and would be passed by the time said decode key is used for decode of contents was memorized. It is characterized by having a license generation means to encipher said decode key and use authorization conditions based on the information on the physical element memorized by said physical element path storage means, and to generate a license.

[0028] since [according to this invention] the information on a physical element that a license would win popularity in order and would be passed by the time a decode key is used for decode of contents was memorized, a decode key and use authorization conditions are enciphered based on the information on the memorized physical element and a license is generated — unjust use of contents — precision — it can prevent highly.

[0029] Moreover, this invention manages the use authorization conditions of these contents with the decode key which decodes the enciphered contents. It is the license management method with which answers a contents use demand from a user, enciphers this decode key and use authorization conditions, and a user is provided as a license. The physical element path registration process of registering the information on a physical element that a license will win popularity in order and will be passed by the time said decode key is used for decode of contents, It is characterized by including the license generation process which enciphers said decode key and use authorization conditions based on the information on the physical element registered according to said physical element path registration process, and generates a license.

[0030] Moreover, this invention manages the use authorization conditions of these contents with the decode key which decodes the enciphered contents. It is the license manager with which answers a contents use demand from a user, enciphers this decode key and use authorization conditions, and a user is provided as a license. The physical element path registration procedure of registering the information on a physical element that a license will win popularity in order and will be passed by the time said decode key is used for decode of contents, It is characterized by performing the license generation procedure which enciphers said decode key and use authorization conditions based on the information on the physical element registered by said physical element path registration procedure, and generates a license by computer.

[0031] since [according to this invention] the information on a physical element that a license would win popularity in order and would be passed by the time a decode key is used for decode of contents was registered, a decode key and use authorization conditions are enciphered based on the information on the registered physical element and a

license is generated — unjust use of contents — precision — it can prevent highly.

[0032]

[Embodiment of the Invention] With reference to an accompanying drawing, the gestalt of suitable operation of the license management equipment concerning this invention, a license management method, and a license manager is explained below.

[0033] Drawing 1 is drawing showing the configuration of the contents use control system which is the gestalt of 1 operation of this invention. The contents use control system 10 shown in drawing 1 is a system which controls this use, when a user 2 uses the contents of the work which the copyright person 1 created. In drawing 1, this contents use control system 10 is large, and has the copyright person system 20, the contents server 30, a license server 40, and the user system 50.

[0034] The copyright person system 20 enciphers the created contents. By sending out a contents decode key required decoding the secrecy contents registration section 21 which performs processing (S10) which registers these enciphered secrecy contents into the contents server 30, and the enciphered contents (secrecy contents) to a license server 40. It has the right transfer section 22 of an access control which performs processing (S12) which transfers the right of an access control to a license server, and the ACL (S14) setting section 23 which sets use authorization conditions (ACL) as a license server 40, and the use control about the contents of a work is managed.

[0035] When the secrecy contents sent from the copyright person system 20 are registered and there is a secrecy contents distribution request from the user system 50 (S16), the contents server 30 is sent out to the user system 50, where these secrecy contents registered and saved are enciphered (S17).

[0036] A license server 40 has license authorization / generation section 41 and the LDAP system 42. License authorization / generation section 41 searches the decode key corresponding to the physical element ID certificate and this which were added to this use demand when there was a use demand of contents from the user system 50 (S18) from the LDAP system 42, a physical element ID decodes, the contents decode key corresponding to the contents by which the use demand was carried out searches, and the license enciphered with the physical element ID in this searched contents decode key transmits (S21).

[0037] This license is physical environmental specification element conditions, is made equivalent to the structure of a physical element, and serves as an OR and a gestalt of the combination structured using the AND. Moreover, with the gestalt of this operation, not only the physical environmental specification element conditions of having been used from the former but the accounting conditions on condition of a user's use situation are collectively enciphered as ACL. About encryption and a decryption of this license, it mentions later. In addition, when the physical element ID certificate is not added to a use demand (S18), in not existing in the LDAP system 42, physical element criteria specification (S19) is sent to the user system 50, and it returns the physical element ID certificate group which the user system 50 generated (S20).

[0038] On the other hand, when the contents decode key by the right transfer of an access control has been sent from the copyright person system 20 (S12), the database of the key 44 in the LDAP system 42 which mentions this contents decode key later is made to correspond to secrecy contents, and it registers with it. Moreover, this ACL is made that an ACL setup has been sent from the copyright person system 20 (S14), and to correspond to secrecy contents, and it stores in the access control list (ACL) in the LDAP system 42.

[0039] The user system 50 has the distribution request (S16) of secrecy contents, secrecy contents demand / acquisition section 51 which acquires the distributed secrecy contents, a demand (S18) of a license, i.e., a use demand, and license demand / acquisition section 52 which processes acquisition (S21) of a license, and the specific use environment (SUE) 53 of a user system. In the specific use environment 53, a specific contents use environment is said and synthetic information, such as CPU, a peripheral device, a RIMUBARU storage, an IC card, and a contents use situation, is said.

[0040] By the specific use environment, it has the use environmental specification physical elements (PCSUE) 54-1, such as CPU, - 54-N, the contents storage device 55-1 which stores contents - 55-M, and the playback devices 56-1, such as a player and a viewer, - 56-L. Each PCSUE 54-1 - 54-N, each contents storage device 55-1 - 55-M, and each playback device 56-1 - 56-L have encryption / decryption / evaluation section 58-1 - 58-N, 60-1 - 60-M, and 62-1 - 62-L while having each physical element ID 57-1 - 57-N, 59-1 - 59-M, and 61-1 - 61-L.

[0041] When enciphering and outputting with the physical element ID of a self-physical element in enciphering each physical element, and decrypting each physical element, encryption / decryption / evaluation section 58-1 - 58-N, 60-1 - 60-M, and 62-1 - 62-L decrypt with the physical element ID of a self-physical element, and performs processing which evaluates a decode result further. That is, about processing of each physical element ID, it carries out for every physical element, and even if it is on the interface between physical elements, he is trying for information not to leak.

[0042] Processing of the copyright person system 20 mentioned above next, the contents server 30, a license server 40, and a user system of operation is explained mainly with reference to a flow chart. First, with reference to the flow chart of drawing 2, the internal-processing procedure of the copyright person system 20 is explained.

[0043] In drawing 2, it judges whether the actuation event generated the copyright person system 20 first (step S100). when the actuation event has not occurred (step S100 — nothing), this processing is repeated until an actuation event occurs, and the contents of actuation of an actuation event judge secrecy contents registration, ACL registration, and the right transfer of an access control for the actuation event to have occurred (step S100 — it is) (step S101).

[0044] When the contents of actuation are secrecy contents registration (step 101, secrecy contents registration),

the secrecy contents registration section 21 enciphers contents (step S110), specifies the desired contents server 30 from a contents server list (step S111), and performs a secrecy contents registration demand to this specified contents server 30 (step S112). Then, the response from the contents server 30 is obtained and it judges whether the response is O.K. or it is an error (step S113).

[0045] When the response from the contents server 30 is O.K., in being an error, after performing error processing (step S114), it judges further whether the following contents server was specified as it is (step S115). when the processing which shifted to step S112 and was mentioned above when the following contents server was specified (step S115 — it is) is repeated and the following contents server is not specified (step S115 — nothing), the processing which shifted to step S100 and was mentioned above is repeated.

[0046] in judging whether the contents decode key as which the ACL setting section 23 was specified further is registered when the contents of actuation are ACL setup (step 101, ACL setup) (step S120), and not registering a contents decode key (step S120 — nothing), error processing is performed (step S124), and it shifts to step S100 and repeats the processing mentioned above. on the other hand, when there is registration of a contents decode key (step S120 — it is), an ACL setting demand is transmitted to a license server 40 (step S122), an ACL registration result is received from a license server 40 (step S123), and the processing which shifted to step S100 after that, and was mentioned above is repeated.

[0047] Moreover, when the contents of actuation are the right transfers of an access control (step S101, right transfer of an access control), the enciphered contents decode key is transmitted to a license server 40 (step S130), the registration result of an encryption contents decode key is received (step S131), it shifts to step S100 and the processing mentioned above is repeated.

[0048] Below, ACL set up by the ACL setting section 23 is explained here. Drawing 3 is drawing showing an example of an access condition, and an access condition has two kinds such as accounting conditions and physical environmental specification element (PCSUE) conditions. As shown in drawing 3, as accounting conditions which are one of the descriptions of this invention, first, there is maxCount (count maximum of operational) and the use situation of the contents corresponding to this is count (operated count). It is going to access control, i.e., limitation, and license by preparing the limit of the count maximum of operational to the adjustable value of an operated count.

[0049] The use situation of the contents corresponding to the accounting condition value of the next maxLength (read-out length between couplings) is totalLen (asked [read die-length +] read-out die length), and tends to control access by the read-out maximum length of contents. The use situation of the contents corresponding to the accounting condition value of the next maxTimeLen (the maximum time amount which can be performed) is totalTime (performed time amount length), and tends to control access by the maximum time amount of contents which can be performed. The use situation of the contents corresponding to the accounting condition value of the next maxDebt (lease possible amount of money (accounting conditions)) is debt (balance), and the minus value of the balance tends to serve as a debt frame, and tends to control access by accounting conditions.

[0050] Moreover, as physical environmental specification element conditions, there is a body of a computer first, and the class of the physical element ID corresponding to this is PSN, and is the serial number of a processor. Here, a class is an object class on a database. The class of the physical element ID corresponding to the following peripheral device is DSN, and shows the class and serial number of a device. The class of the physical element ID corresponding to the following media is MSN, and shows the class and serial number of media. The physical element ID corresponding to the following IC card is certificates, and shows the certificate which an IC card publishes.

[0051] The next body parts are a fingerprint and retina (iris) information, and the class of the physical element ID corresponding to this is bodyParts, and is the authentication information on a body part. The class of the physical element ID corresponding to the time zone which the next permits is timePeriod, and are a local clock and global GPS time of day. The next network domain shows the area on a network, and the class of the physical element ID corresponding to this is MACAddress, and shows a MAC Address. The geographical location of the following shows a use country etc., and the class of the physical element ID corresponding to this is location, and shows the location which GPS or PHS detects. The class of the physical element ID corresponding to storage of the next man is user-ID WithPwd, and shows user ID and a password. The class of the physical element ID corresponding to the last group is group, and shows the set of a physical element ID.

[0052] Such an access condition is set up as a set with a logical combination of AND and OR, i.e., ACL. Although there are accounting conditions and physical environmental specification element conditions in an access condition as mentioned above, combination is possible for these to arbitration. For example, the following is set up as one ACL. That is, ACL like `udac_aclread:(grop=sysrapOR group=soft4soft) (AND45661244<MSN<45661412) OR count<1;modify:user=yujiOR user=hataORIC_card=1afd234fe4def458c3bac78497bbda6 f;print:group=sysrap;` can be set up.

[0053] According to this set-up ACL, "read" shows perusal conditions, and a group is "sysrap" or "soft4soft", and it becomes the conditions for perusal that media serial number MSN exceeds 45661244, and is less than 45661412, or an operated count does not use contents less than one, i.e., once. Furthermore, "modify" shows updating conditions and it becomes the conditions for renewal of contents that a user name is "yuji" or "hata", or the number of "IC_card" is "1afd234fe4def458c3bac78497bbda6f."

[0054] Moreover, "print" can show printout conditions, and a group can restrict it to "sysrap", and it can print contents. The copyright person 1 can set such ACL as arbitration from the copyright person system 20. Operability of this ACL setup improves by using GUI. In addition, you may make it set up the type of ACL with an actuation

name. For example, conditions can be chosen access condition (1) Coming [the actuation name 1], and you may enable it to choose conditions access condition (2) Coming [the actuation name 2]. Thereby, operability improves further.

[0055] Below, with reference to the flow chart shown in drawing 4 , the internal-processing procedure of the contents server 30 is explained. In drawing 4 , first, the contents server 30 judges a secrecy contents registration demand and a secrecy contents distribution request, when a network event is inputted or it is inputted (step S200). when a network event is not inputted (step S200 — nothing), the decision processing in step 200 is repeated.

[0056] When a network event is a secrecy contents registration demand (step S200, secrecy contents registration demand), internal registration of these secrecy contents by which the registration demand was carried out is carried out (step S210), and default ACL is set up (step S211). And the processing which performed the response to this secrecy contents registration demand (step S212), shifted at step S200, and was mentioned above to the copyright person system 20 is repeated.

[0057] On the other hand, when a network event is a secrecy contents distribution request (step S200, secrecy contents distribution request), these secrecy contents by which the distribution request was carried out are distributed to the user system 50 (step S220), the response to this secrecy contents distribution request is performed to the user system 50 after that (step S221), and the processing which shifted to step S200 and was mentioned above is repeated. Thereby, secrecy contents can be distributed to the user system 50 from the copyright person system 20 in the secret condition through the contents server 30. In this case, traffic is distributed, and since it is possible to hold secrecy contents to the contents server near the user system 50 beforehand while fast transfer is possible, distribution processing can be processed at a high speed.

[0058] Below, with reference to the flow chart shown in drawing 5 , the internal-processing procedure of a license server 40 is explained. In drawing 5 , a license server 40 judges first whether the network event of a contents use demand was inputted (step S300). when a network event is not inputted (step S300 — nothing), decision processing of this step S300 is repeated.

[0059] When a network event is a contents use demand (step S300, contents use demand), ACL of the specified contents is searched from the LDAP system 42 (step S301), the access condition related from this searched ACL is extracted further, and new ACL is generated (step S302). When it judges whether there is any correspondence physical element ID certificate corresponding to the physical environmental specification conditions extracted after that (step S303) and there is a correspondence physical element ID certificate (step S303, those with a correspondence physical element ID certificate), as it is When there is no correspondence physical element ID certificate (with step S303 and no correspondence physical element ID certificate) After requiring a certificate from the user system 50 as opposed to the use claimant of contents (step S304), it judges further whether there are any following physical environmental specification conditions (step S305).

[0060] when the preparations which shift to step S303 and are certainly equipped with a correspondence physical element ID certificate when there are the following physical environmental specification conditions (step S305 — it is) are made and there are no following physical environmental specification conditions (step S305 — nothing), a physical element ID certificate group is received (step S306)., the use claimant 50, i.e., the user system, of contents

[0061] Then, license authorization / generation section 41 searches the specified contents decode key (step S307), and re(step S308) arranges the access condition in ACL in the certificate of the physical element which can be forced. Furthermore, processing which bundles all the AND/OR types in ACL with an authentication priority in a parenthesis is performed (step S309). License authorization / generation section 41 performs after that license generation processing which generates a license based on the AND/OR type bundled with this parenthesis (step S310). And the generated license is transmitted to the user system 50 (step S311), and the processing which shifted to step S300 and was mentioned above is repeated.

[0062] Here, the relation of the license and secrecy contents which were generated is explained with reference to drawing 6 . Drawing 6 shows relation with the secrecy contents transmitted to the user system 50 from the copyright person system 20 through the license and the contents server 30 which are transmitted to the user system 50 from a license server 40.

[0063] In drawing 6 , the system ACL 43-1 to 43-5 matched with each secrecy contents 71-75, respectively is stored in ACL43 of a license server 40. The licenses 84-86 over the secrecy contents 71-73 are generated based on this system ACL from the system ACL corresponding to the after that, for example, secrecy, contents 71-73, and it is transmitted to a user system. These licenses 84-86 are enciphered with the corresponding physical element ID, and information does not leak outside. The user system 50 can decode clients 81-ACL 83 from licenses 84-86, can decode secrecy contents 71' corresponding to these - 73', and can obtain contents, respectively.

[0064] In this case, since secrecy contents are also enciphered, security is enough. Thus, ACL and secrecy contents are matched although the transfer roots differ, respectively, maintaining the secrecy condition. In addition, the condition of the secrecy contents sent through the transfer path containing the contents server 30 is expressed as a virtual storing field 70.

[0065] Here, the LDAP system 42 in a license server 40 is further explained with reference to drawing 7 . In drawing 7 , the LDAP system 42 has two or more LDAP servers, a license server 40 will be positioned as the client-server, and each LDAP server will function on the basis of management of a license server 40. A LDAP server is a directory server using the protocol of the lightweight version of DAP contained in X.500 which is the criterion of a directory service. It has the class of the XML information which was divided by two or more classes in the LDAP server, for example, was described by the individual humanity news 91, the system class 92, MEDIAKURASU 93, and

XML.

[0066] And if "own system" is searched in the class of the individual humanity news 91, this system is searched by "system name" from the system class 92, and the present media in the system class 92 "current media" can search MEDIKURASU 93 out of MEDIKURASU, and can retrieve the XML information 94 corresponding to these contents from the contents in this MEDIKURASU 93 further, for example. The information about contents is stored in this XML information 94.

[0067] By the way, the specific use environment of the user system 50 has the logical structure with the layer shown in drawing 8. In drawing 8, the specific use environment 100 consists of three layers of the application layer 110, OS kernel layer 111, and the device layer 112, and it connects between each class with the service interface shown by the dotted line. The application layer 110 has contents playback / activation application 101, and has the secret contents decode protection library 102 as a program module inside.

[0068] The secret contents decode protection library 102 operates the storage driver 103, a file system 105, two or more use environmental specification physical element drivers 106-108, and a playback device driver. The storage driver 103 makes a contents storage device drive, the use environmental specification physical element drivers 106-108 make the use environmental specification physical elements 109-111 drive, respectively, and the playback device driver 112 makes the playback device 113 drive. In addition, it may be one physical unit or two roles, the contents storage device 104 and the use environmental specification element 109, may be borne, for example like MO equipment.

[0069] Drawing 9 shows the correspondence relation between OS kernel layer 111 of a use environmental specification physical element (PCSUE), and the device layer 112. As shown in drawing 9, PCSUE(s) may have inclusion relation. Of course, other devices in the device layer 112 are the same. For example, PCSUE133,134 is positioned by the low order of PCSUE131, and PCSUE135,136 is positioned by the low order of PCSUE134. The data exchange of the information on a physical element ID etc. can be carried out by PCSUE(s) which have such inclusion relation.

[0070] For example, PCSUE of media regenerative apparatus, such as DVD equipment, includes PCSUE of media, such as DVD, and exchanges contents data and media ID information among both. For example, it is information interchange between PCSUE134 and PCSUE135. And only the top PCSUE performs the data exchange with a PCSUE driver. For example, it is the relation between the PCSUE driver 120 and PCSUE131. Therefore, even if it is the same device layer, it may have inclusion relation and may have hierarchical relation.

[0071] As mentioned above, a license is the consent information over a specific environment, and the access information which becomes the client environment which required the license, i.e., the environment of a user system, from ACL and the content decode key Kc only including the information on a proper is enciphered with a physical element ID (PCSUE-ID).

[0072] Here, it is as follows when an example of the multiplexed license is shown. Namely, [Equation 1]

$$\{ \{ \{ \{ \{ \langle \text{アクセス情報} \rangle \} K_5 \} K_4 \} K_3 \} K_2 \} K_1 \}$$

It comes out. Here, K1 - K5 are PCSUE-ID, respectively. Access information is combined for this license by AND conditions using K1 - K5. It is good for the security reinforcement of a physical element to use each PCSUE-ID for high order, and to encipher in multiplex. The sequential decode of this decryption will be carried out from outside PCSUE-ID at this reverse.

[0073] Moreover, when the security reinforcement of a physical element is almost the same, you may enable it to decode each PCSUE-ID by the code key of the result with EXCLUSIVE OR operation. For example, [Equation 2]

$$\{ \langle \text{アクセス情報} \rangle \} (K_5 \oplus K_4 \oplus K_3 \oplus K_2 \oplus K_1)$$

** — it is good to make it like. The effectiveness of diversification of risks that the danger of the contents decode key Kc theft by attack success to some products, i.e., some physical elements, is distributed by multiplexing of these encryption will be brought about.

[0074] Moreover, [Equation 3] when combining two or more PCSUE-ID by the OR-operation child

$$\{ \langle \text{アクセス情報} \rangle \} K_5 + \{ \langle \text{アクセス情報} \rangle \} K_4 +$$

$$\{ \langle \text{アクセス情報} \rangle \} K_3 + \{ \langle \text{アクセス情報} \rangle \} K_2 +$$

$$\{ \langle \text{アクセス情報} \rangle \} K_1$$

** — when like, it is good also considering the value which generated the sublicense enciphered by each PCSUE-ID, { < access information > } K1 [for example,], carried out the OR operation of all the sublicenses simply, and was combined as a license. In this case, multiplexing of the encryption mentioned above may be applied also to each sublicense, and you may generate as a license combined with the nest by carrying out AND, XOR, and an OR operation. The effectiveness of diversification of risks is acquired by this.

[0075] Below, the generation procedure of such a license is explained with reference to the flow chart shown in drawing 10. The flow chart shown in this drawing 10 is the subroutine of the license generation procedure shown in step S310 of drawing 5. In drawing 5, it reads from ACL mentioned above 1 word first (step S400). the WORD read after that — "(" — it is — a ***** is judged (step S410).)

[0076] the WORD which carried out reading appearance — "(" — it is — a case (to step S410 and "("), the read-out current position of ACL is memorized as the starting point in [ACL] a parenthesis (step S411).)) Then, Variable

NB is set as "0" (step S412), and it reads from ACL 1 word further (step S413). then, the read WORD — "(" — it is — a ***** — judging (step S414) — "(" — it is — after adding "1" to Variable NB (step S415), it shifts to step S413 and the following 1 word is again read to a case.))

[0077] on the other hand, it judges whether read-out WORD is "" (" — it is not — a case (step S414 — in addition) — further — this read WORD — ") (step S416). When this read WORD is not "", in addition to this, it comes out, and in a certain case, it shifts to step S413 and 1 word is further read from ACL. On the other hand, when this read WORD is "", it judges whether NB is "0" (step S417). When NB is not "0" (steps S417 and NO), "1" subtraction is carried out from the value of NB, and it shifts to step S413, and reads from ACL 1 word further.

[0078] When NB is "0" (steps S417 and YES), the one this side of the current position of ACL is memorized as a terminal point in [ACL] a parenthesis (step S419). Then, license generation processing in [ACL] this parenthesis is performed (step S420), processing which adds the return value by that recursive call to access condition AC is performed (step S421), and it shifts to step S400. ACL in a parenthesis is generated by this.

[0079] the WORD read on the other hand — "(" — it is not — to a case (step S410 — in addition), it judges further whether this read WORD is physical element conditions or accounting conditions (step S410). In being physical conditions or accounting conditions, this condition is set as access condition AC (step S431), and it sets up as a secret key Kp of a physical element which can force this condition (step S432), shifts to step S400, and reads from ACL 1 word further.

[0080] When the read WORD is not physical conditions or accounting conditions (step S410, in addition to this), it judges further whether this read WORD is "OR" (step S430). When the read WORD is "OR", license generation processing of next ACL is performed from this read WORD (step S441). Then, when it judges whether AC is contained or not (step S442) and AC is contained in the license generated further (steps S442 and YES), it is set as the license which serves as "{hash [AC,] Kp and return value" using the return value of the license generation processing by step S441 (step S443), and this generated license is returned (step S454). On the other hand, when AC is not contained in the license (steps S442 and NO), it is set as the license which serves as "{hash [Kc, AC,] Kp and return value" using the return value of the license generation processing by step S441 (step S445), and this generated license is returned (step S454).

[0081] On the other hand, when the read WORD is not "OR" (step S430, in addition to this), it judges further whether this read WORD is "AND" (step S440). When the read WORD is "AND", license generation processing of next ACL is performed from this read WORD (step S452), and the license which serves as "{hash [a return value, AC,] Kp" using the return value of this license generation processing is returned (step S454).

[0082] Furthermore, when this read WORD is not "AND" (step S440, in addition to this), the license used as "{hash [Kc, AC,] Kp" is returned (step S454). Thereby, a license is generated from ACL.

[0083] Below, with reference to the flow chart shown in drawing 11, the internal-processing procedure of the user system 50 is explained. In drawing 11, it judges first whether the user system 50 had the use demand of contents (step S500). when there is no use demand of contents (step S500 — nothing), this decision processing is repeated, and when there is a use demand of contents (step S500 — it is), the use demand of contents is transmitted (step S501). then, when it judges whether there was any demand of the certificate of a physical element from a license server 40 (step S502) and there is no demand of the certificate of a physical element (step S502 — nothing), it shifts to step S508.

[0084] on the other hand, when there is a demand of the certificate of a physical element (step S502 — it is), it judges whether it read (step S503), and the physical element ID certificate was read and went wrong (step S504). When read-out goes wrong (steps S504 and YES), an error notification is transmitted to a license server (step S505), and it shifts to step S500. when it judges whether there is any following physical element on the other hand when read-out does not go wrong (steps S504 and NO) (step S506) and there is the following physical element (step S506 — it is), it shifts to step S503 and the processing which read the following physical element ID certificate and was mentioned above is repeated.

[0085] on the other hand, when there is no following physical element (step S506 — nothing), a physical element ID certificate group is transmitted to a license server 40 (step S507), and receiving contents judge an error or a license further (step S508). The processing which shifted to step S500 and was mentioned above when receiving contents were errors (step S508, error) is repeated, and when receiving contents are licenses (step S508, license), the processing which shifted and mentioned the license above to the physical element (PCSUE) 1 at delivery (step S509) and step S500 is repeated further. Thereby, the user system 50 can acquire a license from a license server 40.

[0086] Here, PCSUE1 shows PCSUE of the beginning of PCSUE of an individual (N-1), generally PCSUEi shows, and i is 1 - (N-1) an integer. Then, an internal-processing procedure when a license is passed to each PCSUEi is explained with reference to the flow chart of drawing 12.

[0087] In drawing 12, PCSUEi decodes the received license by Kpi first (step 600). Then, this decoded access condition ACi is evaluated (step S601), and it judges whether it is improper whether the evaluation result of an access condition ACi is good (step S602). When the evaluation result of an access condition ACi is improper (step S602, failure), error processing is performed (step S604) and this processing is ended. On the other hand, when the evaluation result of an access condition ACi is good (step S602, C), this decoded license is transmitted to PCSUE (i+1), decode is continued, and internal processing of Book PCSUEi is ended.

[0088] Next, PCSUE (i+1) is equivalent to PCSUE (N), and the physical element of a playback device performs internal processing here, for example. This internal-processing procedure is explained with reference to the flow

chart shown in drawing 13. In drawing 13, the received license is first decoded by Kpn (step S700). Then, this decoded access condition AC(N) is evaluated (step S701), and it judges whether this evaluation result is good or improper (step S702). When an evaluation result is improper (step S702, failure), error processing will be performed (step S703), this processing will be ended, and secrecy contents can be decoded as a result.

[0089] On the other hand, when the evaluation result of access condition AC(N) is good (step S702, C), a playback device reproduces the contents which decoded secrecy contents (step S704) and were decoded by this decoded Kc (step S705), and this processing is ended.

[0090] Here, decode processing of a concrete license is explained with reference to drawing 14. In drawing 14, the license generated by the license server 40 enciphers access control list ACL and a contents decode key using the key Kp which is the physical element ID of the playback device 144, and the value of the exclusive OR of DSN141 which is the device serial number of a storage device, and MSN143 which is the media serial number of media 142 is further enciphered as a key.

[0091] First, if write a storage device 140 in media 142, it reads improper MSN, the exclusive OR of this value and DSN of storage device 140 self is calculated and a license is decoded by this result of an operation, a license will serve as {ACL, Kc} Kp. When satisfying the access condition which this license decoded in part is sent to the playback device 144, and the playback device 144 decodes a license using the key Kp which is the physical element ID which playback device 144 self has, acquires the access condition list ACL and the contents decode key Kc, and access condition ACL shows, the contents which could decode and were decoded by the contents decode key Kc will be reproduced by the playback device 144.

[0092] With reference to the data flow which shows the contents decode processing by the license demand and license acquisition which were mentioned above to drawing 15, it explains further. It sets to drawing 15, and in the decode protected area in the user system 50, in order to use contents first, a physical element ID certificate is attached and the license demand processing 152 is sent out to a license server 40. Under the present circumstances, a physical element ID certificate is acquired from the use environmental specification physical element 150 by the use environmental specification physical element certification dictation profit processing 153, and is passed by the license demand processing 152.

[0093] On the other hand, if a license is transmitted from a license server 40, the license acquisition processing 156 acquires this license, in access-permission processing 155, while acquiring a license from the license income processing 156, a physical element ID will be acquired through the use environmental specification physical element certification dictation profit processing 153, a use situation will be further acquired from accounting 157, and the use environmental specification physical element ID authentication processing 154 will take [processing] out a decode key using these.

[0094] And the contents decode processing 159 decodes the secrecy contents 158 using a contents decode key, and outputs the contents of a plaintext. In addition, accounting 157 is notified to the use situation monitor physical element 151, and the decrement of the current use situation is automatically carried out according to use with the use environment-monitoring physical element 151.

[0095] By the way, drawing 16 is drawing showing the effect of the protection reinforcement on [at the time of mounting each processing procedure in each entity of the specific use environment shown in drawing 8]. From this result, generation of a use environmental specification physical element possession certificate is mounted in a device layer, and understands that it is desirable to mount in the device layer by the IC card for accounting information protection. Thus, since protection reinforcement changes also with layers which mount each processing procedure, it is necessary to mount each processing facility which also takes layer arrangement into consideration and is shown in drawing 15.

[0096] In addition, although the gestalt of operation mentioned above explained as a configuration on the basis of the so-called contents cache possible mold model, it is clear that it is applicable not only to this but the configuration on the basis of a contents coincidence distribution mold model. In this case, the contents server 30 should just deal with it as a configuration by which internal arrangement was carried out into the license server 40.

[0097] Furthermore, what is necessary is to be able to carry either out and just to apply a respectively suitable method according to an adapted system, even if it uses a private key cryptosystem and uses a public key cryptosystem in this case although it is the requisite about encryption and a decryption to use a key with the gestalt of operation mentioned above.

[0098] Moreover, the record medium of portable molds, such as the media used in case not only the equipment of immobilization but this user system 50 is used for the user system 50, i.e., CD-ROM, DVD and MO, an IC card, and a floppy disk, is included in the physical element shown in the gestalt of operation mentioned above. In the user system by which this portable type of record medium is used, in addition to the physical element of immobilization to this user system, this portable type used of record medium will also be contained in a physical element, and use control of contents will be made. In addition, it cannot be overemphasized that it is contained in the physical element which the media of immobilization to the user system 50, for example, the hard disk drive unit of immobilization, ROM of immobilization, etc., mentioned above.

[0099]

[Effect of the Invention] since according to this invention the information on a physical element that a license would win popularity in order and would be passed by the time a decode key is used for decode of contents was memorized, and it constituted so that a decode key and use authorization conditions might be enciphered based on the information on the memorized physical element and a license might be generated as explained above — unjust

use of contents — precision — the effectiveness that it can prevent highly does so.

[0100] moreover — since according to this invention the information on a physical element that a license would win popularity in order and would be passed by the time a decode key is used for decode of contents was registered, and it constituted so that a decode key and use authorization conditions might be enciphered based on the information on the registered physical element and a license might be generated — unjust use of contents — precision — the effectiveness that it can prevent highly is done so.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the contents use control system which is the gestalt of 1 operation of this invention.

[Drawing 2] It is the flow chart which shows the internal-processing procedure of the copyright person system 20 shown in drawing 1 .

[Drawing 3] It is drawing showing an example of accounting conditions and physical environmental specification element conditions.

[Drawing 4] It is the flow chart which shows the internal-processing procedure of the contents server 30 shown in drawing 1 .

[Drawing 5] It is the flow chart which shows the internal-processing procedure of a license server 40 shown in drawing 1 .

[Drawing 6] It is drawing showing relation with the secrecy contents sent from the license and the copyright person system 10 which are sent from a license server 40, or the contents server 30.

[Drawing 7] It is drawing showing the configuration of the LDAP system 42 shown in drawing 1 .

[Drawing 8] It is drawing showing the layer logical structure of a specific use environment.

[Drawing 9] It is drawing showing an example of a physical element with inclusion relation.

[Drawing 10] It is the detail flowchart which shows license generation procedure.

[Drawing 11] It is the flow chart which shows the internal-processing procedure of the user system 50 shown in drawing 1 .

[Drawing 12] It is the flow chart which shows the license decode procedure by the use relation specification physical element.

[Drawing 13] It is the flow chart which shows the license decode procedure by the physical element of a playback device.

[Drawing 14] It is drawing showing an example of the decode process of a license.

[Drawing 15] It is the data flow diagram showing the contents decode processing by a license demand and license acquisition.

[Drawing 16] It is drawing showing the effect of the protection reinforcement on [at the time of mounting each processing procedure in each entity of a specific use environment].

[Drawing 17] It is drawing showing the access-control model in the former.

[Drawing 18] It is drawing showing the outline configuration of the contents use control system corresponding to the access-control model in the former.

[Drawing 19] It is drawing showing the improved access-control model.

[Drawing 20] It is drawing showing the contents distribution model of the contents use control system in the former.

[Drawing 21] It is drawing showing a contents cache possible mold model.

[Drawing 22] It is drawing showing the outline configuration of the contents use control system corresponding to the contents cache possible mold model shown in drawing 21 .

[Drawing 23] It is drawing showing the outline configuration of the contents use control system which realizes a contents coincidence distribution mold model.

[Description of Notations]

1 Copyright Person

2 User

10 Contents Use Control System

20 Copyright Person System

21 Secret Contents Registration Section

22 Right Transfer Section of Access Control

23 ACL Setting Section

30 Contents Server

40 License Server

41 License Authorization / Generation Section

42 LDAP System

43 Access Control List (ACL)

44 Key
50 User System
51 Secrecy Contents Demand / Acquisition Section
52 License Demand / Acquisition Section
53 Specific Use Environment
54-1 - 54-N Use environmental specification physical element
55-1 - 55-M Contents storage device
56-1 - 56-L Playback device
57-1, 59-1, 61-1 Physical element ID
58-1, 60-1, 62-1 Encryption / decryption / evaluation section

[Translation done.]

* NOTICES *

JPO and NCIPJ are not responsible for any damages caused by the use of this translation.

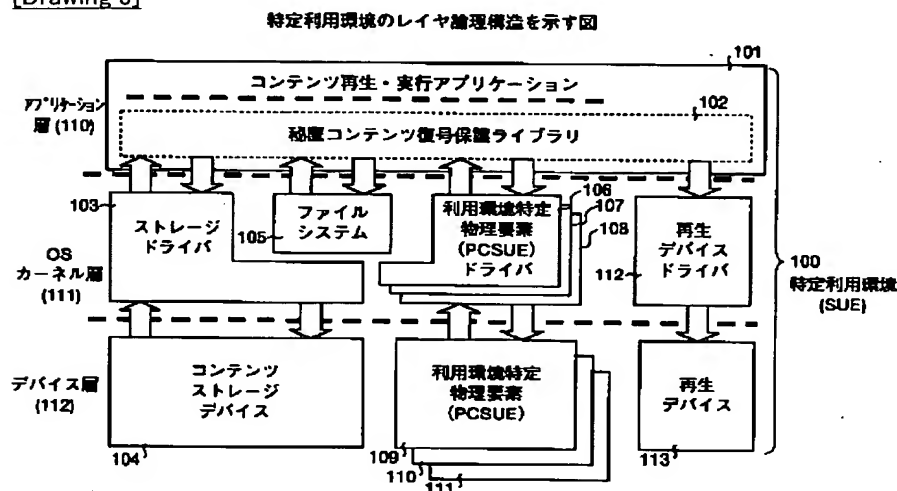
1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

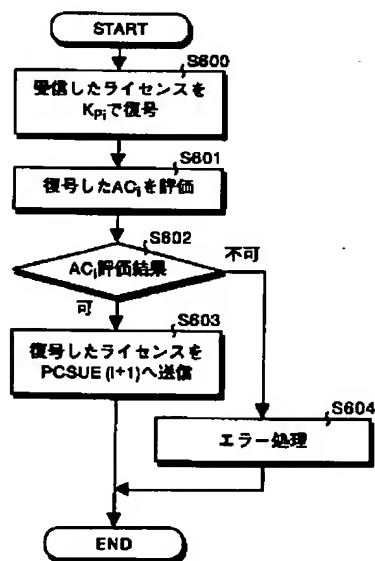
DRAWINGS

[Drawing 8]



[Drawing 12]

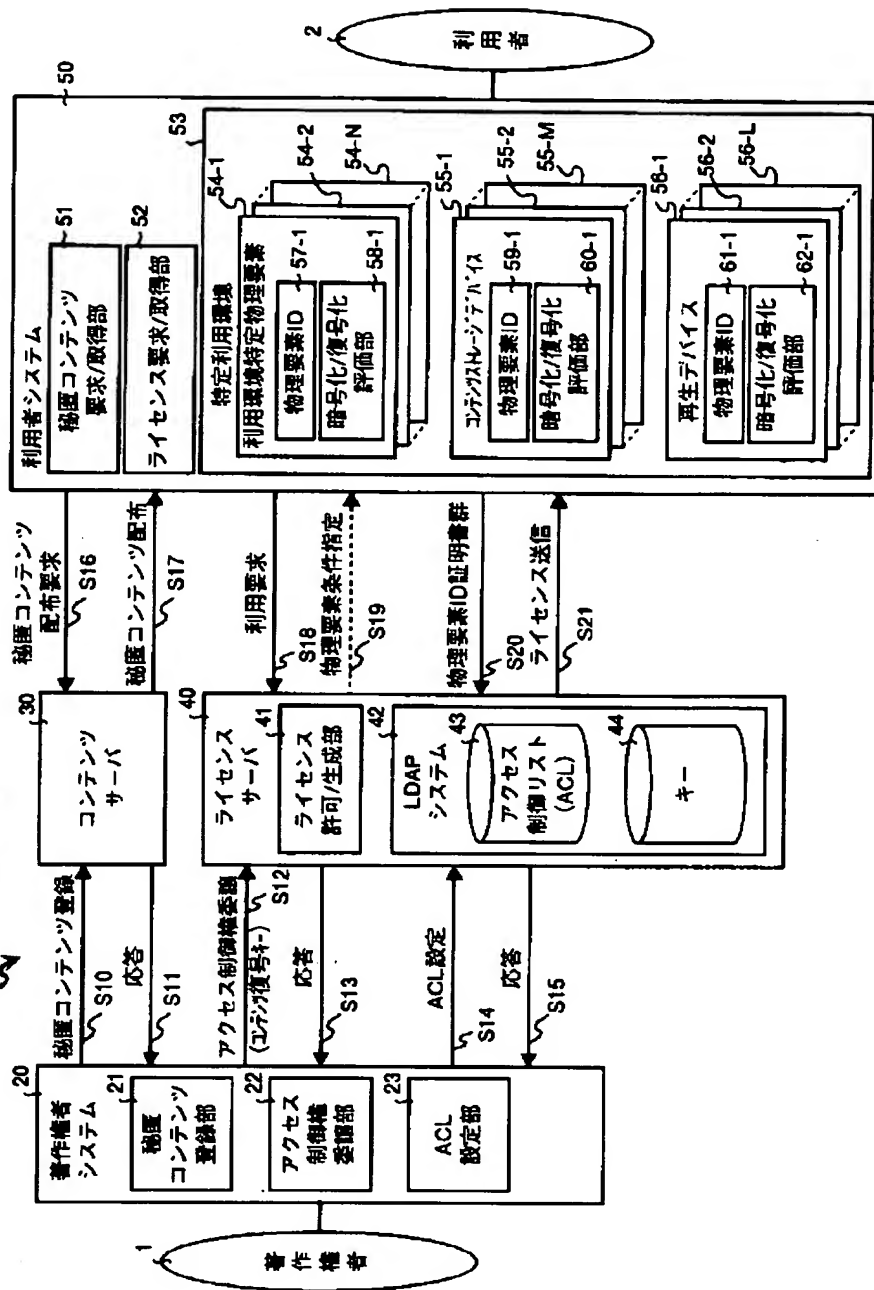
利用者関係特定物理要素によるライセンス
復号処理手順を示すフローチャート



[Drawing 1]

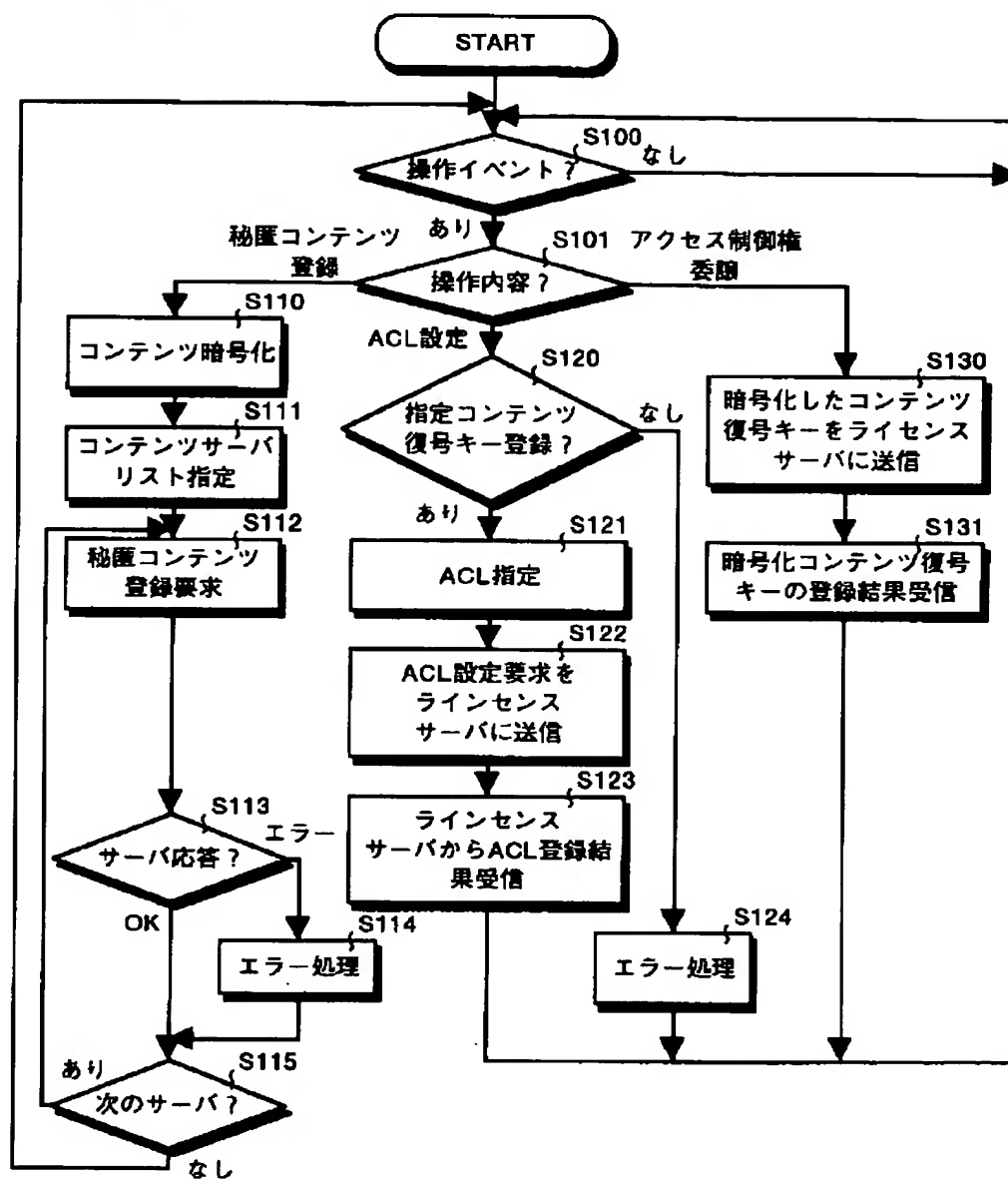
本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図

10 コンテンツ利用制御システム



[Drawing 2]

図1に示した著作権システム20の内部処理手順を示すフローチャート



[Drawing 3]

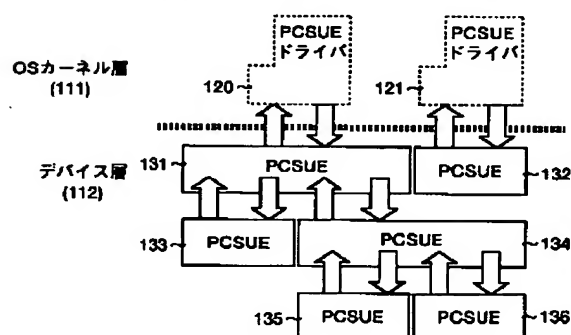
会計条件と物理環境特定要素条件との一例を示す図

会計条件値 (Account Condition Value)	利用状況 (Usage State)
max Count : 操作可能回数最大値	count : 操作済回数
max Length : 読み出し最大長さ	totalLen : 読み出し済長さ + 被要求読み出し長さ
max TimeLen : 実行可能最大時間	totalTime : 実行済時間長
max Debt : 借入可能金額 (課金条件)	debt : 残金 (マイナスは借入金額)

物理環境特定要素 (PCSUE) 条件	物理要素IDクラス (PCSUE-IDClass)
(1) 計算機本体	PSN (プロセッサシリアル番号)
(2) 周辺デバイス	DSN : デバイスの種別、シリアル番号
(3) メディア	MSN : メディアの種別、シリアル番号
(4) ICカード	certificates : ICカードが発行する証明書
(5) 人体部位 (指紋、網膜…)	body Parts : 人体部位 (指紋、網膜…) 認証情報
(6) 許可する時間帯	time Period : 時刻 (ローカルクロック、GPSなど)
(7) ネットワークドメイン	MACAddress : MACアドレス
(8) 地理的位置 (利用国など)	location : GPS/PHS検出位置
(9) 人の記憶	user-ID WithPwd : ユーザIDとパスワード
(10) グループ	group : 物理要素IDの集合

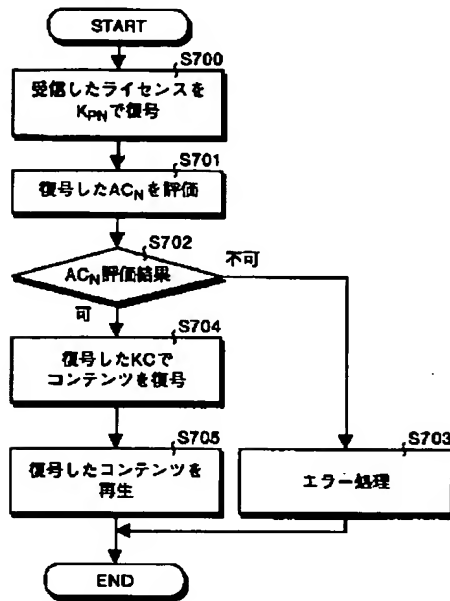
[Drawing 9]

包含関係をもった物理要素の一例を示す図



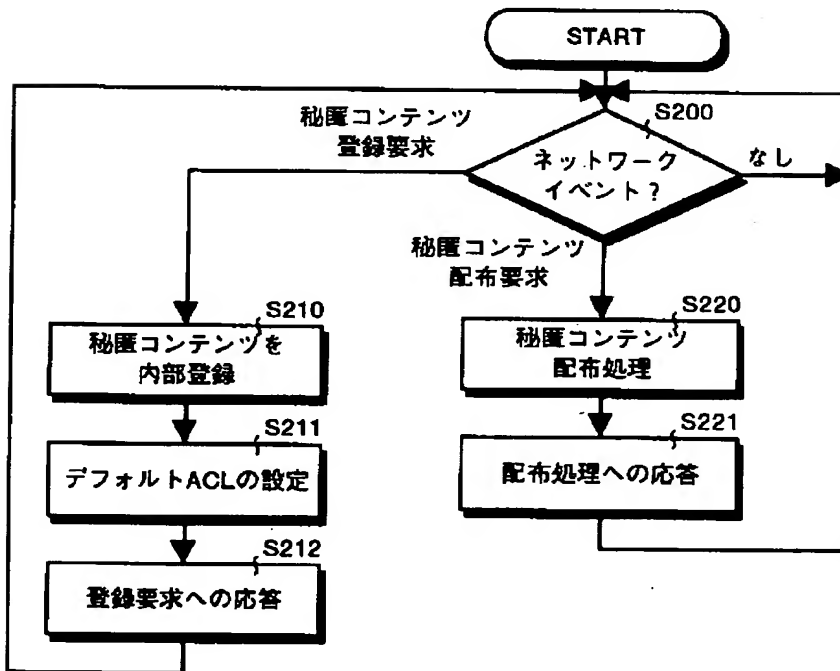
[Drawing 13]

再生デバイスの物理要素によるライセンス
復号処理手順を示すフローチャート

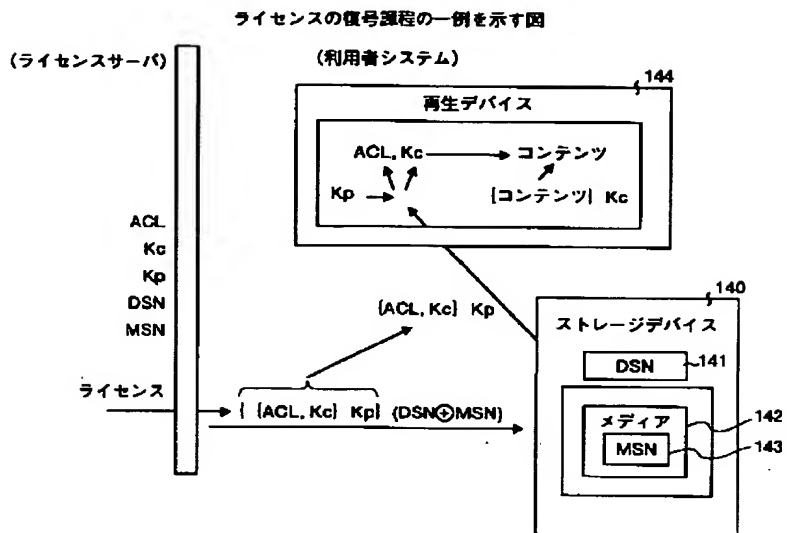


[Drawing 4]

図1に示したコンテンツサーバ30の内部処理手順を示すフローチャート

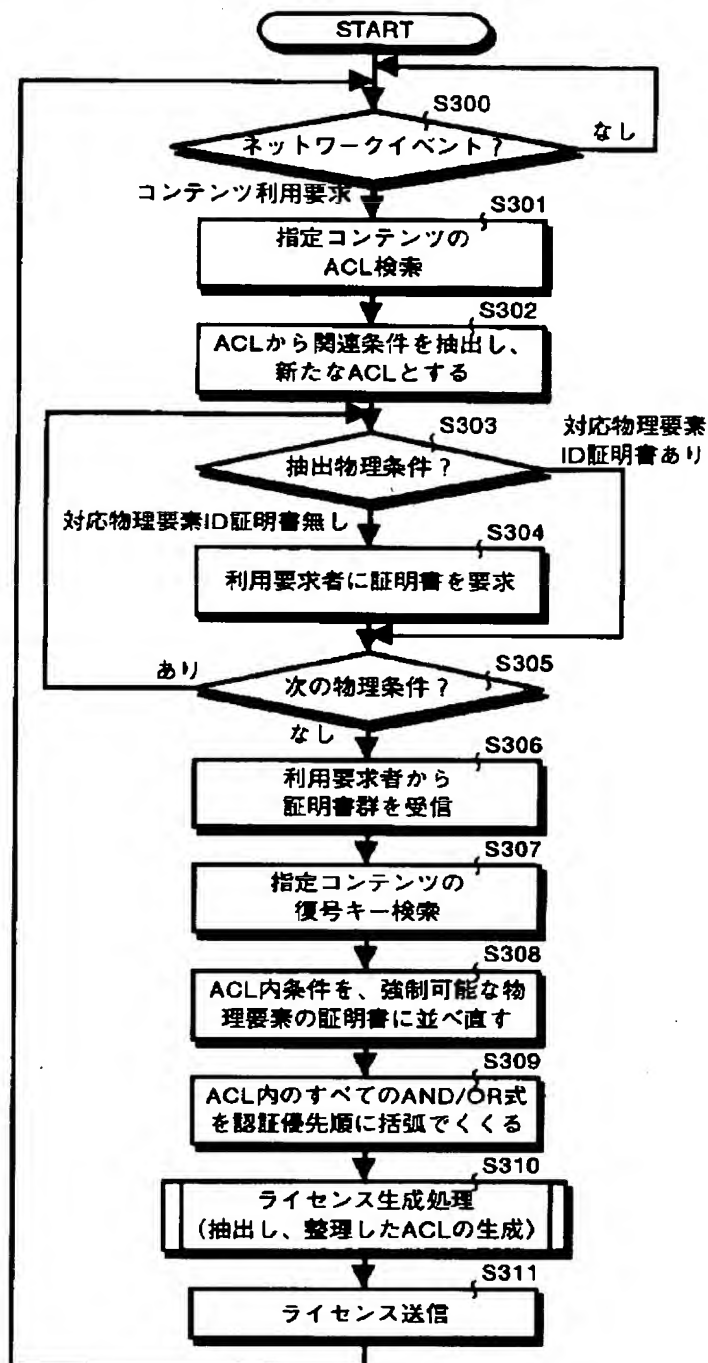


[Drawing 14]



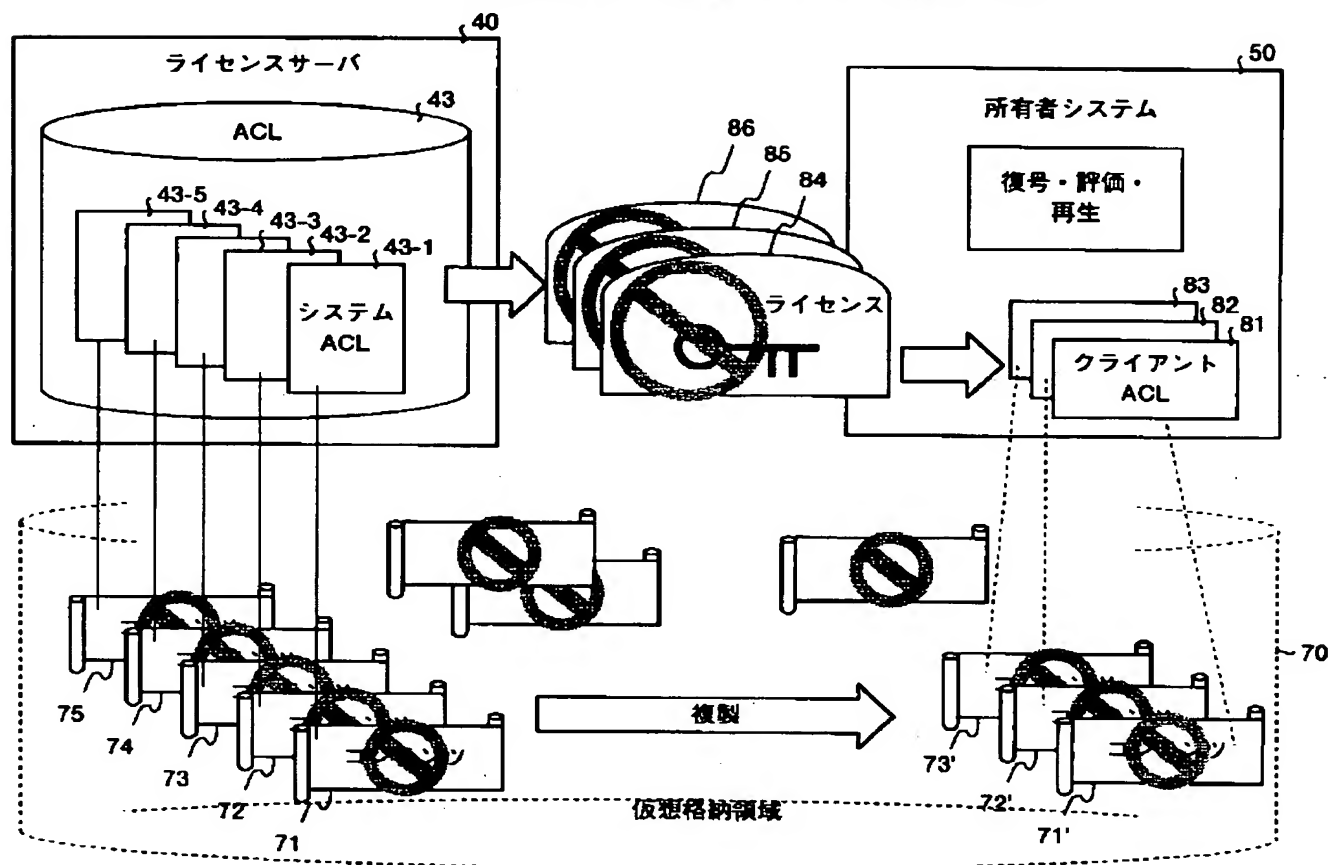
[Drawing 5]

図1に示したライセンスサーバ40の内部処理手順を示すフローチャート



[Drawing 6]

ライセンスサーバ40から送られるライセンスと著作権者システム10あるいは
コンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図



[Drawing 16]

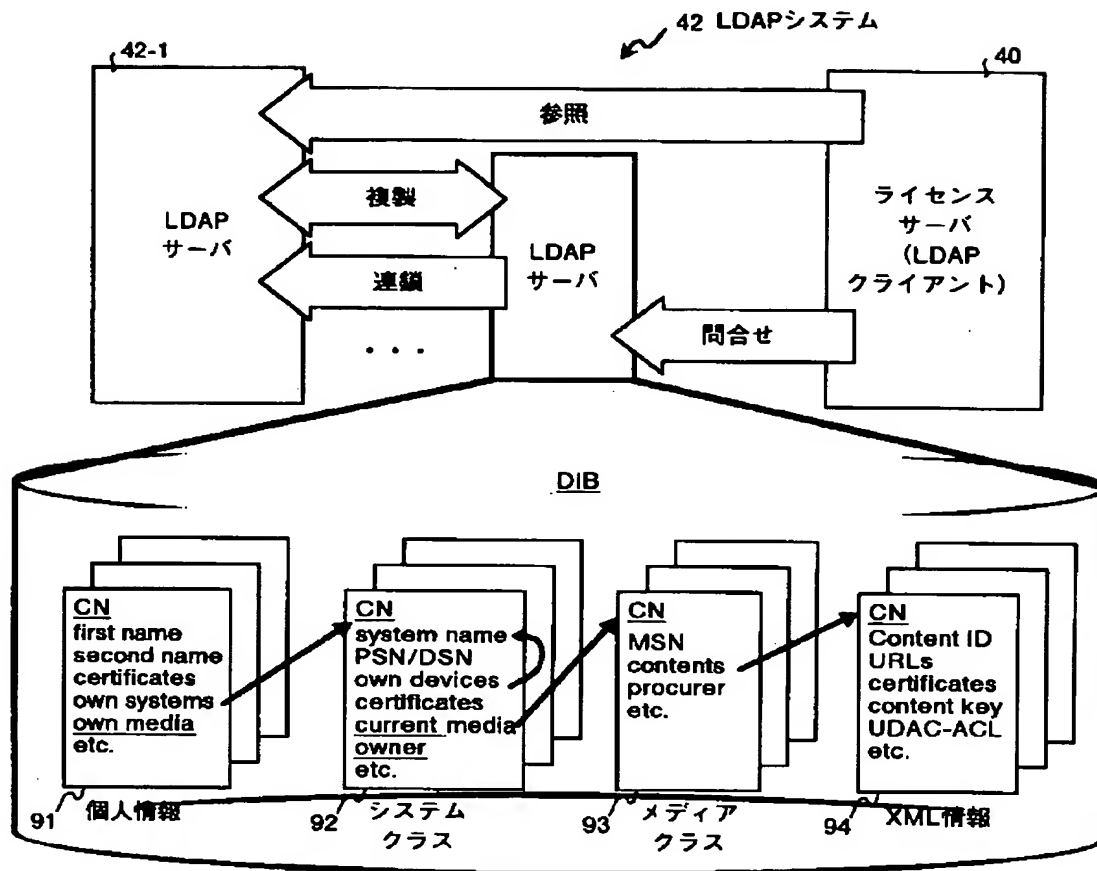
特定利用環境の各エンティティに各処理手続きを
実装した場合における保護強度への影響を示す図

	アプリケーション層	デバイスドライバ層	デバイス層
利用環境特定物理要素 所有証明書生成	—	○	●
利用環境特定物理要素 ID認証	○	—	—
アクセス制御リスト 検索	○	—	○
会計情報保護	△	—	● (ICカード)
条件付アクセス許可	○	—	○
復号	○	—	○

—: 実装の意義が小さい △: 危険 ○: 専門家には保護が弱い ●: 保護が強い

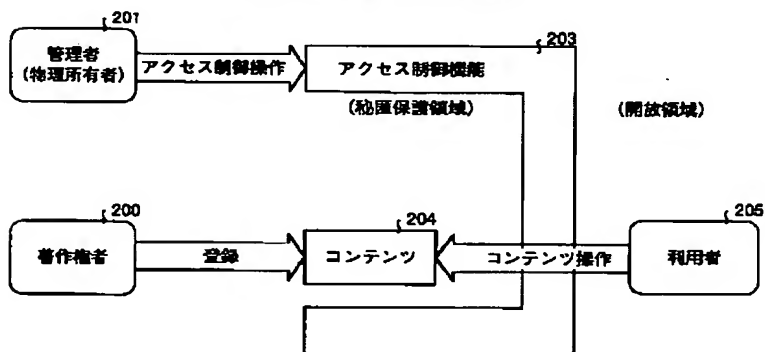
[Drawing 7]

図1に示したLDAPシステム42の構成を示す図



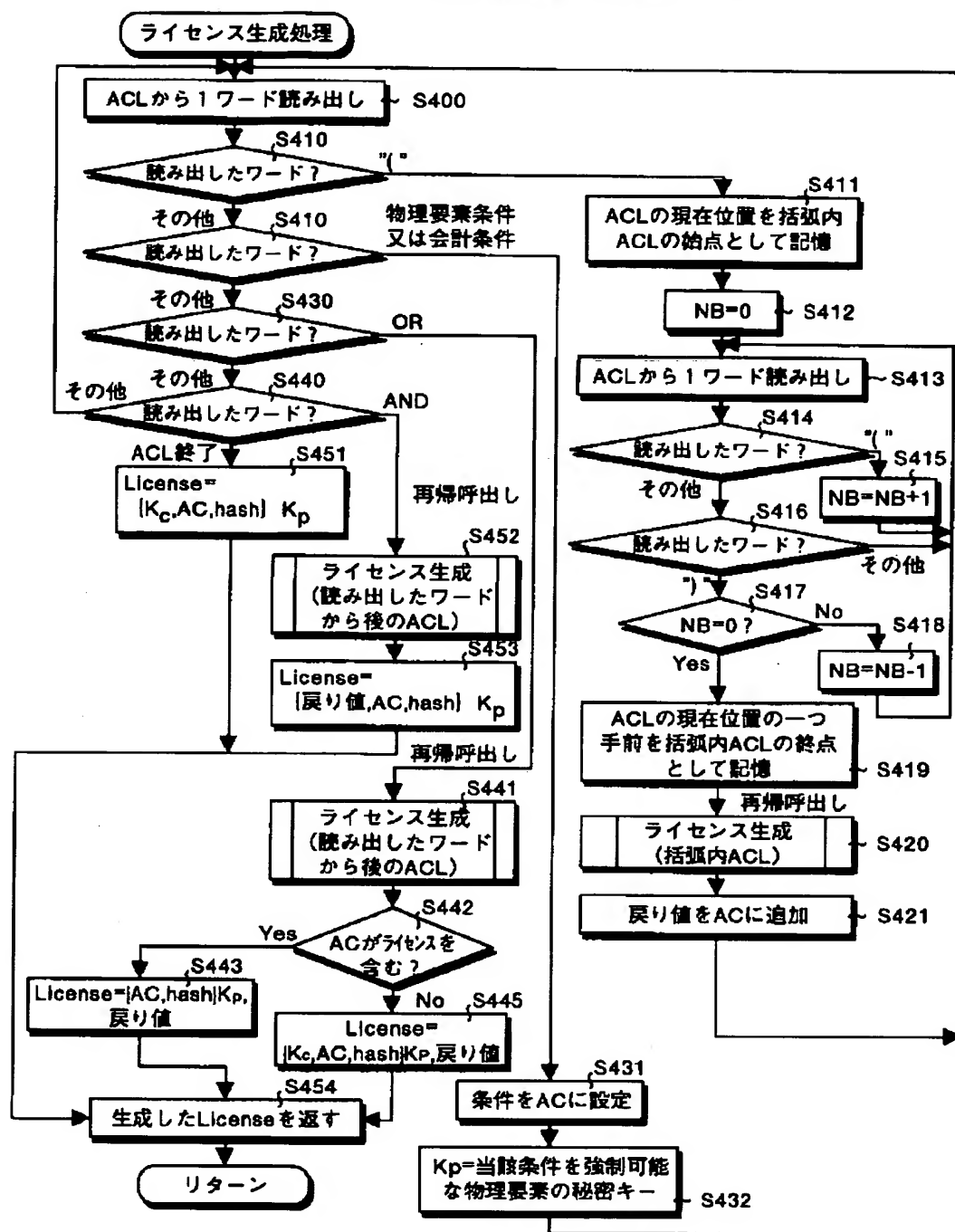
[Drawing 17]

従来のアクセス制御モデルを示す図



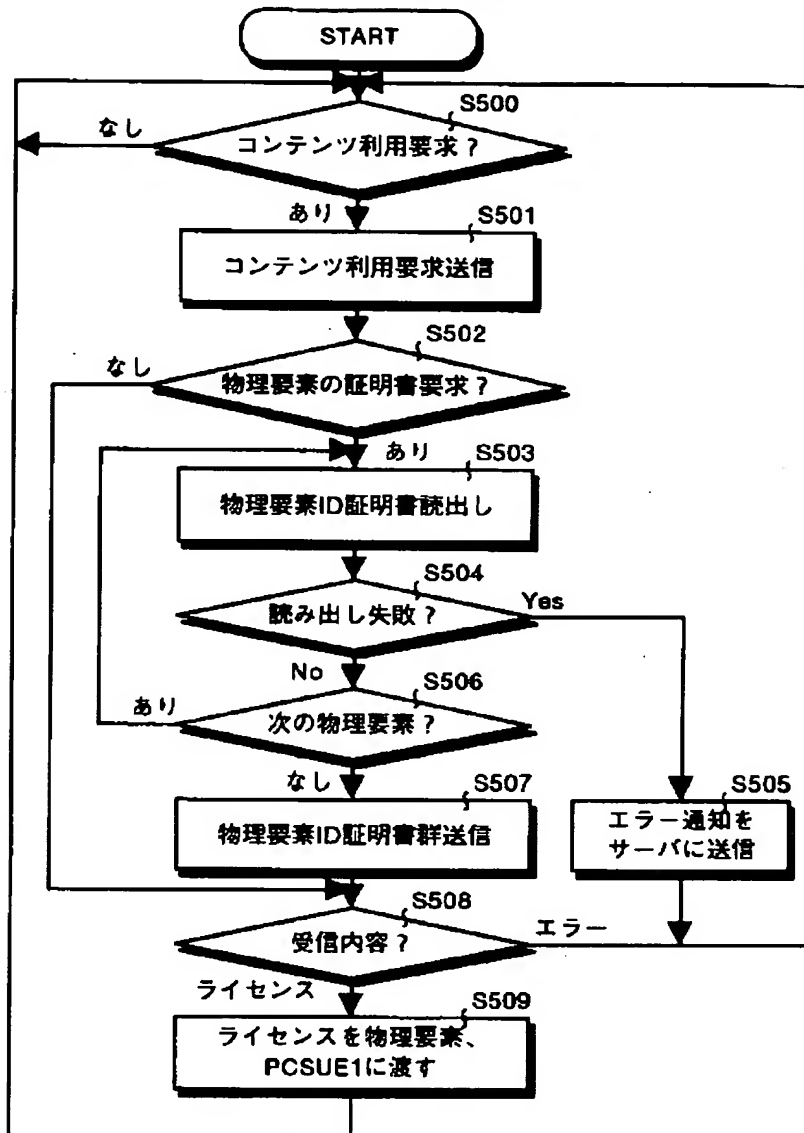
[Drawing 10]

ライセンス生成処理手順を示す詳細フローチャート



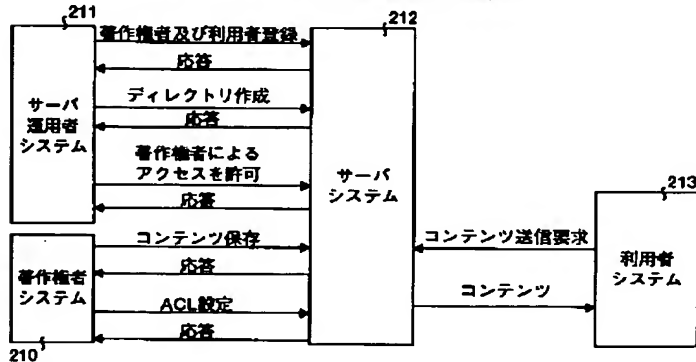
[Drawing 11]

図1に示した利用者システム50の内部処理手順を示すフローチャート



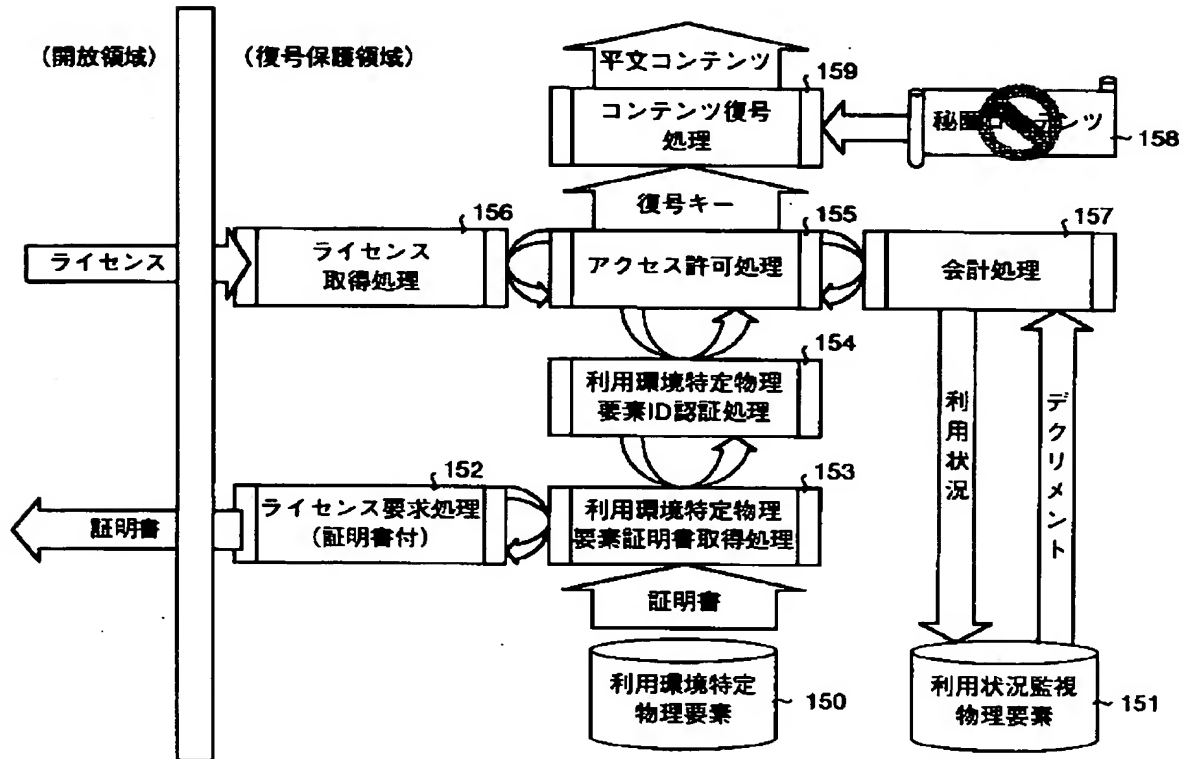
[Drawing 18]

従来のアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図



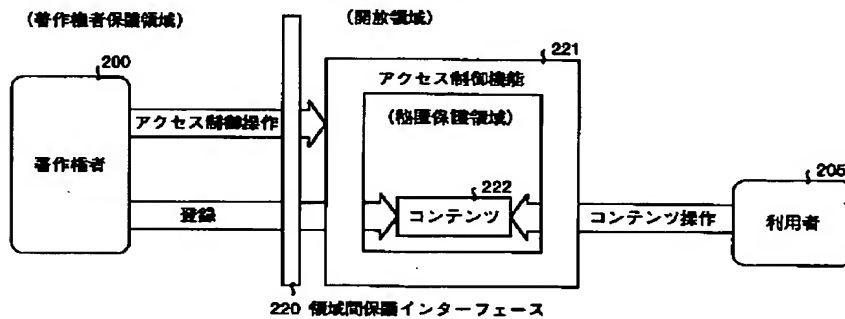
[Drawing 15]

ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図



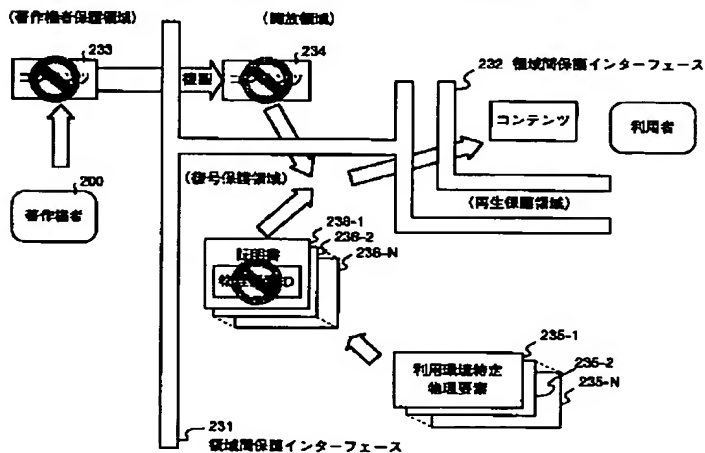
[Drawing 19]

改良したアクセス制御モデルを示す図



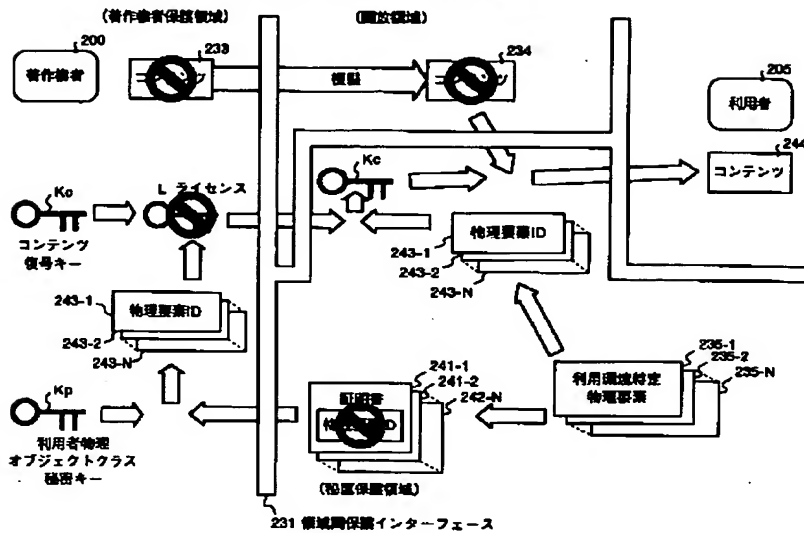
[Drawing 20]

従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図



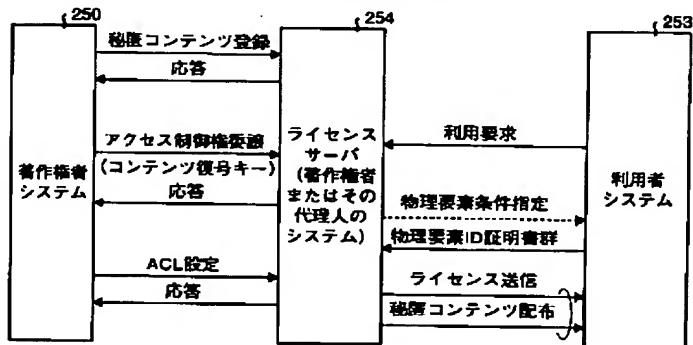
[Drawing 21]

コンテンツキャッシュ可能型モデルを示す図



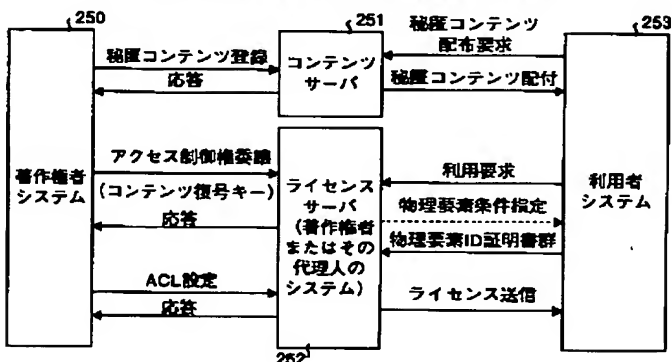
[Drawing 23]

コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図



[Drawing 22]

図21に示したコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示す図



[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-178164

(P2003-178164A)

(43) 公開日 平成15年6月27日 (2003.6.27)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 B 0 8 5
	5 1 2		5 1 2 5 J 1 0 4
12/14	3 2 0	12/14	3 2 0 A
			3 2 0 F

審査請求 有 請求項の数15 O L (全 25 頁) 最終頁に続く

(21) 出願番号 特願2002-270625(P2002-270625)
(62) 分割の表示 特願平11-99482の分割
(22) 出願日 平成11年4月6日(1999.4.6)

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番
1号
(72) 発明者 畠山 卓久
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72) 発明者 吉岡 誠
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(74) 代理人 100089118
弁理士 酒井 宏明

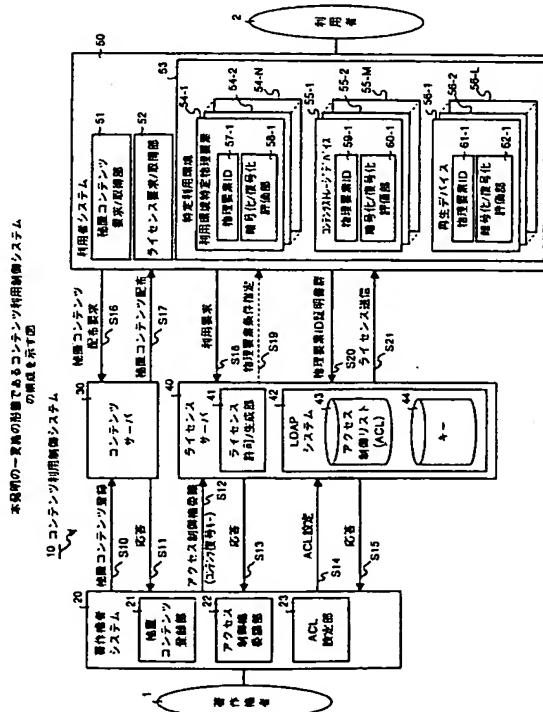
最終頁に続く

(54) 【発明の名称】 ライセンス管理装置、ライセンス管理方法およびライセンス管理プログラム

(57) 【要約】

【課題】 情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができる。

【解決手段】 著作権者システム20とコンテンツサーバ30とライセンスサーバ40と利用者システム50とを有し、著作権者システム20のACL設定部23は、利用者システム50で使用するメディアを含む複数の物理要素のIDおよび利用者IDに基づいてコンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件ACLとして設定し、アクセス制御リスト43に格納する。ライセンスサーバ40は、このアクセス制御リスト43と復号キーKcを複数の物理要素IDを組み合わせで暗号化する。



【特許請求の範囲】

【請求項 1】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に回答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置であって、

前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶した物理要素経路記憶手段と、

前記物理要素経路記憶手段により記憶された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手段と、を備えたことを特徴とするライセンス管理装置。

【請求項 2】 前記物理要素経路記憶手段により記憶された物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成手段は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項 1 に記載のライセンス管理装置。

【請求項 3】 前記ライセンス生成手段は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項 2 に記載のライセンス管理装置。

【請求項 4】 前記物理要素経路記憶手段により固有識別子が記憶された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成手段は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項 2 または 3 に記載のライセンス管理装置。

【請求項 5】 前記ライセンス生成手段は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項 4 に記載のライセンス管理装置。

【請求項 6】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に回答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理方法であって、

前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録工程と、

前記物理要素経路登録工程により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成工程と、を含んだことを特徴とするライセンス管理方法。

【請求項 7】 前記物理要素経路登録工程により登録さ

れた物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成工程は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項 6 に記載のライセンス管理方法。

【請求項 8】 前記ライセンス生成工程は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項 7 に記載のライセンス管理方法。

【請求項 9】 前記物理要素経路記憶工程により固有識別子が記憶された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成工程は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項 7 または 8 に記載のライセンス管理方法。

【請求項 10】 前記ライセンス生成工程は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項 9 に記載のライセンス管理方法。

【請求項 11】 暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に回答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理プログラムであって、

前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録手順と、

前記物理要素経路登録手順により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手順と、をコンピュータで実行することを特徴とするライセンス管理プログラム。

【請求項 12】 前記物理要素経路登録手順により登録された物理要素の情報は、ライセンスが順に受け渡される複数の物理要素の固有識別子を含み、前記ライセンス生成手順は、前記複数の物理要素の固有識別子を組み合わせて前記復号鍵および利用許可条件を暗号化してライセンスを生成することを特徴とする請求項 11 に記載のライセンス管理プログラム。

【請求項 13】 前記ライセンス生成手順は、前記利用許可条件を構成する要素条件のうちそれぞれの物理要素が強制可能な要素条件を、該それぞれの物理要素が受け取ったライセンスから固有識別子を用いて復号可能な形態で暗号化することを特徴とする請求項 12 に記載のライセンス管理プログラム。

【請求項 14】 前記物理要素経路登録手順により固有

識別子が登録された複数の物理要素は、記録媒体、記録装置および再生装置であり、前記ライセンス生成手順は、前記記録媒体、記録装置および再生装置が有する固有識別子に基づいて暗号化することを特徴とする請求項 12 または 13 に記載のライセンス管理プログラム。

【請求項 15】 前記ライセンス生成手順は、前記再生装置の固有識別子を用いて暗号化した後、前記記録媒体の固有識別子と記録装置の固有識別子の排他的論理和を用いて暗号化することを特徴とする請求項 14 に記載のライセンス管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化されたコンテンツを復号する復号鍵とともにコンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に回答して復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムに関する。

【0002】貨幣の役割は、その貨幣という物質としての性質によって、公平な報酬を人々に提供する。貨幣というオブジェクトは、単なる口約束の共有概念ではなく、物理的に存在し、携帯でき、さらに発行元以外による偽造が困難であることが必須要件であった。物理的に存在し、携帯できることによって、その価値の利用者どうしで公平に確認することができ、偽造の困難性によって、その公平な確認の契機を公平なる貨幣の発行元がコントロールすることができた。しかし、近年の工業技術の発展によって、今や貨幣の偽造困難性が崩壊する日が近い。貨幣に代わる新たな価値確認オブジェクトが必要になっている。そのオブジェクトはやはり、まず物理的に存在し、携帯でき、偽造困難である必要がある。さらにそのオブジェクトは発行元がアクセスコントロールできる必要がある。

【0003】このセキュリティ強化面からの要求に加え、情報流通の多様化と大容量化、高速化の側面から「超流通」の実現の要求も高まっている。この「超流通」を実現した環境は、つぎの条件を満足する。すなわち、(1) 情報利用者は、デジタル情報をほぼ無料で入手できること、(2) 情報提供者は、その情報の利用を許可する条件(課金、改変利用条件など)を指定し、利用者の合意した条件を強制することができること、(3) このサービスを利用するに当たって、必要な情報利用者の追加操作は「アクセス条件の確認」程度であること、である。

【0004】こうした超流通のアクセス制御を正確かつ、安全に実行可能なシステムは、ライセンス料などの著作権料徴収の不公平の是正にも寄与することが期待できる。現行システムでは、著作物が相当数売れないと提供者は利益を上げられないが、正確に著作権者の手に渡

るようにシステムを構築できることが望まれる。また、専門家的芸術家から、部品としての創作を提供するデザイナーに至るまで、各人のサービス料に見合う報酬が公平に分配されることが望まれる。

【0005】

【従来の技術】従来、著作物等のコンテンツに対するアクセスを分散システム環境、特に開放ネットワーク上において制御する場合、コンテンツの利用者からのアクセスが可能なサーバにコンテンツを格納し、このサーバに対するアクセスを制御することによって、コンテンツの利用を制御していた。ここで、コンテンツとは、単一の記憶装置媒体に記録可能なビット列の集合としての構造をもつデジタルコンテンツであり、文書テキスト、画像、動画、プログラムソフトウェア等を含む。

【0006】たとえば、図 17 は、従来のアクセス制御モデルを示す図である。図 17 において、コンテンツ 204 は、アクセス制御機能 203 を介してのみ、利用者 205 からのコンテンツ操作を可能としている。また、著作権者 200 は、コンテンツ 204 をアクセス制御機能 203 で保護された、たとえばサーバに登録するのみで、著作権者 200 以外の者、たとえばこのサーバを管理する管理者によってアクセス制御機能 203 に対するアクセス制御操作がなされていた。

【0007】すなわち、図 18 に示すようにコンテンツを保持するサーバシステム 212 は、管理者 201 によって管理運用されるサーバ運用者システム 211 によって管理され、サーバ運用者システム 211 は、サーバシステム 212 に対して著作権者および利用者登録を行い、またこのためのディレクトリ生成を行い、さらに、著作権者によるアクセス制御を許可することも行う。著作権者システム 210 は、著作権者の著作物のコンテンツをサーバシステム 212 に保存させ、アクセス制御条件(ACL)をサーバシステム 212 に対して設定する。この場合、著作権者は、サーバシステム 212 に対してアクセス制御の許可を得なければならない。一方、利用者システム 213 は、コンテンツの利用に際して、コンテンツ送信要求をサーバシステム 212 に対して行い、ACL を満足する場合には、サーバシステム 212 内に保存されていたコンテンツを取得する。

【0008】しかし、コンテンツの利用者にすべての権限が与えられ、移動やコピー(複製)によって利用者が変わると、移動あるいはコピー先のコンテンツに対しては、もとの著作権者の権限はまったく動かない。また、コンテンツオブジェクトを保存するサーバ管理者と著作権者の間では、オブジェクトに対するアクセス許諾強制のあり方も明確ではなく、たとえばサーバ管理者が著作権者に断りなく、アクセス権を変更可能なことが当然のこととされていた。

【0009】一方、近年の記憶媒体等の低価格化等によって分散システム環境が促進され、ネットワークのトラ

フィックが集中することなく、コンテンツを複数のサーバにキャッシュして分散できるようになり、コンテンツオブジェクトに対するアクセスを高速に行うことができるようになった。従って、図 17 に示すようなアクセス制御モデルは、利用者 205 によるコンテンツ操作への入り口のみに対して強固なアクセス制御機能を構築すればよいが、上述した分散システム環境下では、全方向的なアクセス制御あるいはセキュリティ保護を行う必要があった。

【0010】そこで、図 19 に示すようなアクセス制御モデルが考えられた。このアクセス制御モデルでは、著作権者 200 が従来のセキュリティ技術で保護が可能な領域である著作権者保護領域と、あらゆる外部からの攻撃を受容する開放領域と、ハード／ソフトの改ざんの保護とデジタルデータ複製防止処理が施される秘匿保護領域とに分離される。秘匿保護領域は、全方向的なアクセス制御機能 221 によって保護し、このアクセス制御機能 221 内にコンテンツ 222 が保存される。

【0011】このコンテンツに対して、著作権者 200 は、コンテンツ 222 の登録とともに、アクセス制御機能 221 に対するアクセス制御操作も可能としている。利用者 205 は、開放領域から、アクセス制御機能 221 を介してコンテンツ 222 を取得することになる。なお、領域間保護インターフェース 220 は、著作権者保護領域と開放領域との間の保護を行うインターフェースである。

【0012】この図 19 に示す分散システム環境下におけるアクセス制御モデルの具体化は、米国特許 5339403 号公報に記載されており、また、特開平 9-134311 号公報、米国特許 5392351 号公報、米国特許 555304 号公報、および米国特許 5796824 号公報には、利用者の機器をチェックしてコンテンツの不正利用を防止する技術が記載されている。以下、これらの公報を参照して従来のコンテンツ利用制御システムについて説明する。

【0013】図 20 は、従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。図 20 において、復号保護領域と再生保護領域とは、図 18 に示す秘匿保護領域に相当し、復号保護領域は、ハード／ソフトの改ざんの保護と出力データの複製防止保護の領域であり、再生保護領域は、デジタル復号データの複製防止の領域である。利用環境特定物理要素 (PCSUE) 235-1~235-N は、コンテンツの利用環境を特定する物理要素であり、具体的には、CPU、周辺装置、リムーバブルな記憶媒体、IC カード等である。

【0014】復号保護領域では、PCSUE 235-1~235-N に対応する物理要素 ID の証明書 236-1~236-N をもとに、著作権者 200 によって暗号化されたコンテンツ 233 の複製であって開放領域のサーバに存在するコンテンツ 234 を復号し、再生保護領

域を介して、この複合されたコンテンツが利用者に利用される。従って、コンテンツは、物理要素 ID に対応したキーで暗号化され (コンテンツ 233)、このコンテンツ 233 に対応するコンテンツ 234 を復号するためには、各物理要素 ID またはそれに対応した秘密のキーが必要となる。

【0015】ここで、コンテンツ配布モデルには、暗号化されたコンテンツを復号するために用いられるライセンスを、暗号化されたコンテンツと同時に配布するライセンス同時モデルと、暗号化されたコンテンツをサーバのキャッシュに保存し、ライセンスとは別のタイミングで取得するコンテンツキャッシュ可能型モデルとがある。図 21 は、このコンテンツキャッシュ可能型モデルを示す図である。

【0016】図 21 において、まず著作権者 200 は、著作権者保護領域で、コンテンツを生成し、このコンテンツを暗号化し、その後、複製して開放領域のサーバ等にキャッシュされる。一方、PCSUE 235-1~235-N の物理要素 ID を暗号化した証明書 241-1~241-N は、暗号化された状態で著作権者保護領域に出力され、PCSUE 235-1~235-N に対応する利用者物理オブジェクトクラスから秘密キー Kp を取り出し、この秘密キー Kp と証明書 241-1~241-N とから物理要素 ID 243-1~243-N を復号し、この物理要素 ID 243-1~243-N によってコンテンツ復号キー Kc を暗号化し、秘密保護領域に出力する。

【0017】秘密保護領域では、暗号化されたコンテンツ復号キー Kc を物理要素 ID 242-1~242-N で復号し、コンテンツ復号キー Kc を得る。このコンテンツ復号キー Kc を用いて開放領域から取得される、暗号化されたコンテンツ 234 を復号し、コンテンツ 244 として利用者 205 に利用させる。

【0018】図 22 は、図 21 に示すコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示すブロック図である。図 22 において、著作権者システム 250 は、著作権者保護領域に存在し、コンテンツサーバ 251 は、開放領域に存在し、ライセンスサーバ 252 および利用者システム 253 は、秘匿保護領域に存在する。著作権者システム 250 は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ 251 に保存しておく。

【0019】また、コンテンツ復号キー Kc をライセンスサーバ 252 に送信して、アクセス制御権の委譲をライセンスサーバ 252 に対して行う。さらに、アクセス制御リスト (ACL) 設定を行う。利用者システム 253 は、コンテンツを利用することを示す利用要求をライセンスサーバ 252 に送信し、このとき、物理要素 ID の証明群が添付されていない場合には、ライセンスサ

バ252の物理要素条件指定によって物理要素IDの証明群を取得し、ライセンスサーバ252に送出する。

【0020】ライセンスサーバ252は、図21に示したように、利用者の物理オブジェクトクラスの秘密キーKpを取得して物理要素ID証明群を復号し、復号した物理要素IDによって暗号化されたコンテンツ復号キーKcがライセンスLとして利用者システム253に送出される。これによって、利用者システム253の物理要素IDが一致すれば、復号が行われ、この復号されたコンテンツ復号キーKcを用いて秘匿コンテンツを復号することができる。

【0021】なお、秘密コンテンツはコンテンツサーバ251に保存されているので、利用者システム253は、別途コンテンツサーバ251に秘密コンテンツ配布要求を行って、コンテンツサーバ251から秘密コンテンツの配布を受ける必要がある。

【0022】一方、図23は、コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成ブロック図を示している。図23では、コンテンツサーバ251が存在せず、ライセンス送信と同時に利用者システム253に送付されることになる。図22に示すように、コンテンツサーバ251を介して秘密コンテンツを取得する場合、秘密コンテンツは予め時間的に利用者システム253に近いサーバまで運ばれているので、利用者システム253は、コンテンツが必要な時に利用要求をすればよい。

【0023】また、コンテンツ同時配布型モデルに比較してコンテンツの流通経路の適切な選択が可能となり、利用者にとっては、コンテンツ取得に際して応答時間の短縮が期待できる。また、コンテンツキャッシュ可能型モデルでは、コンテンツを、ライセンスの提供とは別に、ROM媒体ベース、放送、Proxyサーバによるキャッシュ等によって、予め配布しておくことが可能であり、利点が多い。

【0024】

【発明が解決しようとする課題】しかしながら、上述した従来のコンテンツ利用制御システムでは、利用者システムに固有の物理要素IDに一致する装置であれば、基本的に秘匿コンテンツを復号でき、このコンテンツを利用することができるが、この物理要素IDのみによってライセンス（利用許可条件）を生成しているので、たとえば、著作権者の意思で決定されるコンテンツの読み出し回数を制限する条件を付加したり、時間制限を設けたり、課金条件を設定したりすることができず、柔軟なコンテンツ利用制御ができないという問題点があった。

【0025】また、利用環境特定物理要素は、常に単純な構成となつてとは限らず、複雑な構成をもった機器である場合には、その機器のうちの特定の機器あるいは部品が不正である場合もあり、このような場合に、単に大きな構成の機器である利用環境特定物理要素によって

利用許可条件を生成しても、不正を見逃してしまうこととなりセキュリティが低下するという問題点があった。

【0026】この発明は上記に鑑みてなされたもので、著作権者等の情報作成者に許諾された者を含む情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができるライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムを提供することを目的とする。

【0027】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に应答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理装置であって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶した物理要素経路記憶手段と、前記物理要素経路記憶手段により記憶された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手段と、を備えたことを特徴とする。

【0028】この発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶し、記憶した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成することとしたので、コンテンツの不正利用を精度高く防止することができる。

【0029】また、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に应答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理方法であって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録工程と、前記物理要素経路登録工程により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成工程と、を含んだことを特徴とする。

【0030】また、本発明は、暗号化されたコンテンツを復号する復号鍵とともに該コンテンツの利用許可条件を管理し、利用者からのコンテンツ利用要求に应答して該復号鍵および利用許可条件を暗号化してライセンスとして利用者に提供するライセンス管理プログラムであって、前記復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録する物理要素経路登録手順と、前記物理要素経路登録手順により登録された物理要素の情報に基づいて前記復号鍵および利用許可条件を暗号化してライセンスを生成するライセンス生成手順と、をコンピュータで実行すること

を特徴とする。

【0031】かかる発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録し、登録した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成することとしたので、コンテンツの不正利用を精度高く防止することができる。

【0032】

【発明の実施の形態】以下に添付図面を参照して、本発明にかかるライセンス管理装置、ライセンス管理方法およびライセンス管理プログラムの好適な実施の形態を説明する。

【0033】図1は、本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。図1に示すコンテンツ利用制御システム10は、著作権者1が作成した著作物のコンテンツを利用者2が利用する場合に、この利用を制御するシステムである。図1において、このコンテンツ利用制御システム10は、大きく、著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、および利用者システム50を有する。

【0034】著作権者システム20は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ30に登録する(S10)処理を行う秘匿コンテンツ登録部21、暗号化したコンテンツ(秘匿コンテンツ)を復号するのに必要なコンテンツ復号キーをライセンスサーバ40に送出することによって、アクセス制御権をライセンスサーバに委譲する(S12)処理を行うアクセス制御権委譲部22、および利用許可条件(ACL)をライセンスサーバ40に設定する(S14)ACL設定部23を有し、著作物のコンテンツに関する利用制御を管理する。

【0035】コンテンツサーバ30は、著作権者システム20から送られた秘匿コンテンツを登録し、利用者システム50からの秘匿コンテンツ配布要求があった(S16)場合に、この登録され、保存されている秘匿コンテンツを暗号化された状態で利用者システム50に送出する(S17)。

【0036】ライセンスサーバ40は、ライセンス許可/生成部41とLDAPシステム42とを有する。ライセンス許可/生成部41は、利用者システム50からコンテンツの利用要求があった(S18)場合、この利用要求に付加された物理要素ID証明書とこれに対応する復号キーをLDAPシステム42から検索し、物理要素IDを復号し、利用要求されたコンテンツに対応するコンテンツ復号キーを検索し、この検索したコンテンツ復号キーを物理要素IDで暗号化したライセンスを送信する(S21)。

【0037】このライセンスは、物理環境特定要素条件であり、物理要素の構造に対応させ、論理和と論理積を用いて構造化した組み合わせの形態となっている。ま

た、この実施の形態では、従来から用いられていた物理環境特定要素条件のみならず、利用者の利用状況を条件とした会計条件も併せてACLとして暗号化される。このライセンスの暗号化と復号化については後述する。なお、利用要求(S18)に物理要素ID証明書が付加されていない場合、LDAPシステム42内にも存在しない場合には、物理要素条件指定(S19)を利用者システム50に送付して、利用者システム50が生成した物理要素ID証明書群を返す(S20)。

【0038】一方、著作権者システム20からアクセス制御権委譲によるコンテンツ復号キーが送られてきた(S12)場合は、このコンテンツ復号キーを後述するLDAPシステム42内のキー44のデータベースに秘匿コンテンツに対応させて登録する。また、著作権者システム20からACL設定が送られてきた(S14)には、このACLを秘匿コンテンツに対応させて、LDAPシステム42内のアクセス制御リスト(ACL)に格納する。

【0039】利用者システム50は、秘匿コンテンツの配布要求(S16)と配布された秘匿コンテンツの取得を行う秘匿コンテンツ要求/取得部51と、ライセンスの要求、すなわち利用要求(S18)とライセンスの取得(S21)の処理を行うライセンス要求/取得部52と、利用者システムの特定利用環境(SUE)53とを有する。特定利用環境53とは、特定のコンテンツ利用環境をいい、CPU、周辺装置、リムーバブルな記憶媒体、ICカード、コンテンツ利用状況などの総合的情報をいう。

【0040】特定利用環境には、CPU等の利用環境特定物理要素(PCSUE)54-1~54-Nと、コンテンツを格納するコンテンツストレージデバイス55-1~55-Mと、プレーヤやビューワ等の再生デバイス56-1~56-Lとを有する。各PCSUE54-1~54-N、各コンテンツストレージデバイス55-1~55-M、および各再生デバイス56-1~56-Lは、それぞれの物理要素ID57-1~57-N、59-1~59-M、61-1~61-Lを有するとともに、暗号化/復号化/評価部58-1~58-N、60-1~60-M、62-1~62-Lを有する。

【0041】暗号化/復号化/評価部58-1~58-N、60-1~60-M、62-1~62-Lは、各物理要素を暗号化する場合には、自物理要素の物理要素IDで暗号化して出力し、各物理要素の復号化を行う場合には、自物理要素の物理要素IDで復号化を行い、さらに復号結果を評価する処理を行う。すなわち、各物理要素IDの処理に関しては各物理要素毎に行い、物理要素間のインターフェース上であっても、情報が漏れないようにしている。

【0042】つぎに上述した著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、利用者シ

システムの動作処理を主としてフローチャートを参照して説明する。まず、図2のフローチャートを参照して、著作権者システム20の内部処理手順について説明する。

【0043】図2において、著作権者システム20は、まず操作イベントが発生したか否かを判断する(ステップS100)。操作イベントが発生していない場合(ステップS100、なし)には、操作イベントが発生するまでこの処理を繰り返し、操作イベントが発生した(ステップS100、あり)には、操作イベントの操作内容が秘匿コンテンツ登録か、ACL登録か、アクセス制御権委譲かを判断する(ステップS101)。

【0044】操作内容が秘匿コンテンツ登録である場合(ステップ101、秘匿コンテンツ登録)には、秘匿コンテンツ登録部21は、コンテンツの暗号化を行い(ステップS110)、コンテンツサーバリストから所望のコンテンツサーバ30を指定し(ステップS111)、この指定したコンテンツサーバ30に対して秘匿コンテンツ登録要求を行う(ステップS112)。その後、コンテンツサーバ30からの応答を得て、その応答がOKであるかエラーであるかを判断する(ステップS113)。

【0045】コンテンツサーバ30からの応答がOKの場合にはそのまま、エラーである場合には、エラー処理を行った(ステップS114)後、さらに、つぎのコンテンツサーバが指定されたか否かを判断する(ステップS115)。つぎのコンテンツサーバが指定された場合(ステップS115、あり)には、ステップS112に移行して上述した処理を繰り返し、つぎのコンテンツサーバが指定されていない場合(ステップS115、なし)には、ステップS100に移行して上述した処理を繰り返す。

【0046】操作内容がACL設定である場合(ステップ101、ACL設定)、ACL設定部23は、さらに、指定されたコンテンツ復号キーを登録するか否かを判断し(ステップS120)、コンテンツ復号キーの登録をしない場合(ステップS120、なし)には、エラー処理を行って(ステップS124)、ステップS100に移行し、上述した処理を繰り返す。一方、コンテンツ復号キーの登録がある場合(ステップS120、あり)には、ACL設定要求をライセンスサーバ40に送信し(ステップS122)、ライセンスサーバ40からACL登録結果を受信し(ステップS123)、その後ステップS100に移行して上述した処理を繰り返す。

【0047】また、操作内容がアクセス制御権委譲である場合(ステップS101、アクセス制御権委譲)には、暗号化したコンテンツ復号キーをライセンスサーバ40に送信し(ステップS130)、暗号化コンテンツ復号キーの登録結果を受信し(ステップS131)、ステップS100に移行し、上述した処理を繰り返す。

【0048】つぎに、ここで、ACL設定部23によ

て設定されるACLについて説明する。図3は、アクセス条件の一例を示す図であり、アクセス条件は、会計条件と物理環境特定要素(PCSUE)条件との2種類がある。図3に示すように、本発明の特徴の一つである会計条件としては、まず、maxCount(操作可能回数最大値)があり、これに対応するコンテンツの利用状況はcount(操作済回数)である。操作済回数という可変値に対して操作可能回数最大値という制限を設けてアクセスを制御、すなわち限定と認可を行おうとするものである。

【0049】つぎのmaxLength(読み出し最大長さ)の会計条件値に対応するコンテンツの利用状況は、totalLen(読み出し済長さ+被請求読み出し長さ)であり、コンテンツの読み出し最大長さによってアクセスの制御をしようとするものである。つぎのmaxTimeLen(実行可能最大時間)の会計条件値に対応するコンテンツの利用状況は、totalTime(実行済時間長)であり、コンテンツの実行可能最大時間によってアクセスの制御をしようとするものである。つぎのmaxDebt(借入可能金額(課金条件))の会計条件値に対応するコンテンツの利用状況は、debt(残金)であり、残金のマイナス値は借入金額となり、課金条件によってアクセスの制御をしようとするものである。

【0050】また、物理環境特定要素条件としては、まず計算機本体があり、これに対応する物理要素IDのクラスは、PSNであり、プロセッサのシリアル番号である。ここで、クラスとはデータベース上のオブジェクトクラスである。つぎの周辺デバイスに対応する物理要素IDのクラスは、DSNであり、デバイスの種類とシリアル番号を示す。つぎのメディアに対応する物理要素IDのクラスは、MSNであり、メディアの種類とシリアル番号を示す。つぎのICカードに対応する物理要素IDは、certificatesであり、ICカードが発行する証明書を示す。

【0051】つぎの人体部位は、たとえば指紋や網膜(アイリス)情報であり、これに対応する物理要素IDのクラスは、bodyPartsであり、人体部位の認証情報である。つぎの許可する時間帯に対応する物理要素IDのクラスは、timePeriodであり、ローカルクロックやグローバルなGPS時刻である。つぎのネットワークドメインは、ネットワーク上のエリアを示し、これに対応する物理要素IDのクラスは、MACAddressであり、MACアドレスを示す。つぎの地理的位置は、利用国などを示し、これに対応する物理要素IDのクラスは、locationであり、GPSあるいはPHSが検出する位置を示す。つぎの人の記憶に対応する物理要素IDのクラスは、user-ID WithPwdであり、ユーザIDとパスワードを示す。最後のグループに対応する物理要素IDのクラスは、groupであり、物理要素IDの集合を示す。

【0052】このようなアクセス条件は、ANDとOR

との論理的な組み合わせをもったセット、すなわちACLとして設定される。アクセス条件には、上述したように会計条件と物理環境特定要素条件とがあるが、これらは任意に組み合わせ可能である。たとえば、一つのACLとしては、つぎのようなものが設定される。すなわち、

```
udac_acl
read:((grop=sysrap OR group=soft4soft) AND
45661244<MSN<45661412) OR count<1;
modify:user=yuji OR user=hata OR
IC_card=1afd234fe4def458c3bac78497bbda6f;
print:group=sysrap;
```

のようなACLを設定することができる。

【0053】この設定されたACLによれば、「read」は閲覧条件を示し、グループが「sysrap」あるいは「soft4soft」であり、かつ、メディアシリアル番号MSNが45661244を越え45661412未満であるか、あるいは操作済回数が1未満すなわち、一度もコンテンツを利用したことがないことが閲覧のための条件となる。さらに、「modify」は更新条件を示し、ユーザ名が「yuji」あるいは「hata」であるか、あるいは「IC_card」の番号が「1afd234fe4def458c3bac78497bbda6f」であることがコンテンツ更新のための条件となる。

【0054】また、「print」は印刷出力条件を示し、グループが「sysrap」に限り、コンテンツを印刷することができる。このようなACLは、著作権者システム20から著作権者1が任意に設定することができる。このACL設定は、GUIを用いることによって操作性が向上する。なお、ACLのタイプは、操作名とともに設定するようにしてもよい。たとえば、操作名1に対してはアクセス条件(1)なる条件を選択でき、操作名2に対してはアクセス条件(2)なる条件を選択できるようにしてもよい。これにより、さらに操作性が向上する。

【0055】つぎに、図4に示すフローチャートを参照して、コンテンツサーバ30の内部処理手順について説明する。図4において、まずコンテンツサーバ30は、ネットワークイベントが入力されたか、入力された場合に秘匿コンテンツ登録要求か、秘匿コンテンツ配布要求かを判断する(ステップS200)。ネットワークイベントが入力されない場合(ステップS200、なし)には、ステップ200における判断処理を繰り返す。

【0056】ネットワークイベントが秘匿コンテンツ登録要求である場合(ステップS200、秘匿コンテンツ登録要求)には、この登録要求された秘匿コンテンツを内部登録し(ステップS210)、デフォルトのACLを設定する(ステップS211)。そして、著作権者システム20に、この秘匿コンテンツ登録要求に対する応答を行って(ステップS212)、ステップS200に移行し、上述した処理を繰り返す。

【0057】一方、ネットワークイベントが秘匿コンテ

ンツ配布要求である場合(ステップS200、秘匿コンテンツ配布要求)には、この配布要求された秘匿コンテンツを利用者システム50に対して配布し(ステップS220)、その後、この秘匿コンテンツ配布要求に対する応答を利用者システム50に対して行い(ステップS221)、ステップS200に移行して上述した処理を繰り返す。これにより、コンテンツサーバ30を介して秘匿コンテンツを秘密状態で著作権者システム20から利用者システム50に配布することができる。この場合、トラフィックが分散され、高速転送が可能であるとともに、予め利用者システム50の近傍のコンテンツサーバまで秘匿コンテンツを保持することが可能であるので、配布処理を高速に処理することができる。

【0058】つぎに、図5に示すフローチャートを参照して、ライセンスサーバ40の内部処理手順について説明する。図5において、まず、ライセンスサーバ40は、コンテンツ利用要求のネットワークイベントが入力されたか否かを判断する(ステップS300)。ネットワークイベントが入力されない場合(ステップS300、なし)には、このステップS300の判断処理を繰り返す。

【0059】ネットワークイベントがコンテンツ利用要求である場合(ステップS300、コンテンツ利用要求)には、指定されたコンテンツのACLをLDAPシステム42から検索し(ステップS301)、さらに、この検索したACLから関連するアクセス条件を抽出し、新たなACLを生成する(ステップ302)。その後抽出した物理環境特定条件に対応する対応物理要素ID証明書があるか否かを判断し(ステップS303)、対応物理要素ID証明書がある場合(ステップS303、対応物理要素ID証明書あり)にはそのまま、対応物理要素ID証明書が無い場合(ステップS303、対応物理要素ID証明書無し)には、コンテンツの利用要求者に対して、すなわち利用者システム50に対して証明書を要求した(ステップS304)後、さらに、つぎの物理環境特定条件があるか否かを判断する(ステップS305)。

【0060】つぎの物理環境特定条件がある場合(ステップS305、あり)には、ステップS303に移行して対応物理要素ID証明書を確実に備える準備をし、つぎの物理環境特定条件がない場合(ステップS305、なし)には、コンテンツの利用要求者、すなわち利用者システム50から物理要素ID証明書群を受信する(ステップS306)。

【0061】その後、ライセンス許可/生成部41は、指定されたコンテンツ復号キーを検索し(ステップS307)、ACL内のアクセス条件を、強制可能な物理要素の証明書に並べ直す(ステップS308)。さらに、ACL内のすべてのAND/OR式を認証優先順に括弧でくくる処理を行う(ステップS309)。その後ライ

センス許可／生成部41は、この括弧でくくられたAND/OR式をもとに、ライセンスを生成するライセンス生成処理を行う（ステップS310）。そして、生成されたライセンスを利用者システム50に送信し（ステップS311）、ステップS300に移行して上述した処理を繰り返す。

【0062】ここで、生成されたライセンスと秘匿コンテンツとの関係について図6を参照して説明する。図6は、ライセンスサーバ40から利用者システム50に送信されるライセンスとコンテンツサーバ30を介して著作権者システム20から利用者システム50に送信される秘匿コンテンツとの関係を示している。

【0063】図6において、ライセンスサーバ40のACL43内には、それぞれ各秘匿コンテンツ71～75と対応づけられたシステムACL43-1～43-5が格納されている。このシステムACLをもとにその後、たとえば秘匿コンテンツ71～73に対応するシステムACLから秘匿コンテンツ71～73に対するライセンス84～86が生成され、利用者システムに送信される。このライセンス84～86は、対応する物理要素IDで暗号化されており、外部に情報が漏れることはない。利用者システム50は、ライセンス84～86からクライアントACL81～83を復号し、これらに対応する秘匿コンテンツ71'～73'を復号し、それぞれコンテンツを得ることができる。

【0064】この場合、秘匿コンテンツも暗号化されているので、セキュリティは十分である。このようにして、ACLと秘匿コンテンツとはその秘匿状態を維持しながら、それぞれ転送ルートが異なるものの、対応づけられている。なお、コンテンツサーバ30を含む転送経路を介して送られる秘匿コンテンツの状態は、仮想格納領域70として表現している。

【0065】ここで、さらにライセンスサーバ40内のLDAPシステム42について図7を参照して説明する。図7において、LDAPシステム42は、複数のLDAPサーバを有し、そのクライアントサーバとしてライセンスサーバ40が位置づけられ、ライセンスサーバ40の管理のもとに各LDAPサーバが機能することになる。LDAPサーバとは、ディレクトリサービスの標準であるX.500に含まれるDAPの軽量版のプロトコルを用いたディレクトリサーバである。LDAPサーバ内には複数のクラスに分けられ、たとえば個人情報91、システムクラス92、メディアクラス93、XMLで記述されたXML情報のクラスを有する。

【0066】そして、たとえば個人情報91のクラスにおいて、「own system」が検索されると、このシステムをシステムクラス92から「system name」によって検索し、さらにシステムクラス92内の現メディア「current media」は、メディアクラスの中からメディアクラス93を検索し、さらに、このメディアクラス93内の

コンテンツから、このコンテンツに対応したXML情報94を検索することができる。このXML情報94の中には、コンテンツに関する情報が格納されている。

【0067】ところで、利用者システム50の特定利用環境は、図8に示すレイヤを持った論理構造を有している。図8では、特定利用環境100が、アプリケーション層110とOSカーネル層111とデバイス層112との3層で構成され、各層間は、点線で示すサービスインターフェースで接続される。アプリケーション層110は、コンテンツ再生・実行アプリケーション101を有し、内部には、秘密コンテンツ復号保護ライブラリ102をプログラムモジュールとして有する。

【0068】秘密コンテンツ復号保護ライブラリ102は、ストレージドライバ103、ファイルシステム105、複数の利用環境特定物理要素ドライバ106～108、再生デバイスドライバを動作させる。ストレージドライバ103は、コンテンツストレージデバイスを駆動させ、利用環境特定物理要素ドライバ106～108はそれぞれ利用環境特定物理要素109～111を駆動させ、再生デバイスドライバ112は再生デバイス113を駆動させる。なお、一つの物理装置であっても、たとえばMO装置のようにコンテンツストレージデバイス104と利用環境特定要素109の二つの役割を担ってもよい。

【0069】図9は、利用環境特定物理要素（PCSUE）のOSカーネル層111とデバイス層112との対応関係を示している。図9に示すように、PCSUEどうしは、包含関係を持つことがある。もちろん、デバイス層112における他のデバイスも同様である。たとえば、PCSUE131の下位にはPCSUE133、134が位置づけられ、PCSUE134の下位にはPCSUE135、136が位置づけられる。このような包含関係を有するPCSUEどうしでは、物理要素ID等の情報をデータ交換することができる。

【0070】たとえば、DVD装置等のメディア再生装置のPCSUEは、DVD等のメディアのPCSUEを包含しており、コンテンツデータやメディアID情報を両者間で交換する。たとえば、PCSUE134とPCSUE135との間の情報交換である。そして、最上位のPCSUEのみがPCSUEドライバとのデータ交換を行う。たとえば、PCSUEドライバ120とPCSUE131との関係である。従って、同じデバイス層であっても、包含関係を有し、階層的な関係を有する場合がある。

【0071】ライセンスは、上述したように、特定環境に対する許諾情報であり、ライセンスを要求したクライアント環境、すなわち利用者システムの環境に固有の情報のみを含むものであり、ACLとコンテンツ復号キーKcとからなるアクセス情報を物理要素ID（PCSUE-ID）によって暗号化されたものである。

【0072】ここで、多重化されたライセンスの一例を示すと、つぎようになる。すなわち、

【数1】

$$\{ \{ \{ \{ \{ \langle \text{アクセス情報} \rangle \mid K_5 \mid K_4 \mid K_3 \mid K_2 \mid K_1 \} \} \} \}$$

である。ここで、 $K_1 \sim K_5$ は、それぞれPC SUE-IDである。このライセンスは、アクセス情報は $K_1 \sim K_5$ を用いてAND条件によって結合されている。物理要素のセキュリティ強度が高い順に各PC SUE-IDを用いて多重的に暗号化するとよい。この復号化は、この逆に外側のPC SUE-IDから順次復号されることになる。

【0073】また、物理要素のセキュリティ強度がほぼ同一の場合には、各PC SUE-IDを排他的論理和演算によってその結果の暗号キーによって復号できるようにしてもよい。たとえば、

【数2】

$$\{ \langle \text{アクセス情報} \rangle \mid (K_5 \oplus K_4 \oplus K_3 \oplus K_2 \oplus K_1) \}$$

のようになるとよい。これらの暗号化の多重化によって、一部の製品、すなわち一部の物理要素への攻撃成功によるコンテンツ復号キーKc盗難の危険性が分散されるという、リスク分散の効果をもたらすことになる。

【0074】また、複数のPC SUE-IDをOR演算子で結合する場合、すなわち、

【数3】

$$\{ \langle \text{アクセス情報} \rangle \mid K_5 + \{ \langle \text{アクセス情報} \rangle \mid K_4 + \{ \langle \text{アクセス情報} \rangle \mid K_3 + \{ \langle \text{アクセス情報} \rangle \mid K_2 + \{ \langle \text{アクセス情報} \rangle \mid K_1 \} \} \} \}$$

のような場合には、それぞれのPC SUE-IDで暗号化されたサブライセンス、たとえば、 $\{ \langle \text{アクセス情報} \rangle \mid K_1$ を生成し、すべてのサブライセンスを単純にOR演算して結合した値をライセンスとしてもよい。この場合、上述した暗号化の多重化を各サブライセンスにも適用し、AND、XOR、OR演算を入れ子にして組み合わせたライセンスとして生成してもよい。これによっても、リスク分散の効果は得られる。

【0075】つぎに、このようなライセンスの生成処理手順について図10に示すフローチャートを参照して説明する。この図10に示すフローチャートは、図5のステップS310に示すライセンス生成処理手順のサブルーチンである。図5において、まず、上述したACLから1ワード読み出す(ステップS400)。その後読み出したワードが「(」であるか否かを判断する(ステップS410)。

【0076】読み出したワードが「(」である場合(ステップS410、「(」)には、ACLの読み出し現在位置を括弧内ACLの始点として記憶する(ステップS411)。その後、変数NBを「0」に設定し(ステッ

プS412)、さらにACLから1ワード読み出す(ステップS413)。その後、読み出したワードが「(」であるか否かを判断し(ステップS414)、「(」である場合には、変数NBに「1」を加算した(ステップS415)後、ステップS413に移行して再び、つぎの1ワードを読み出す。

【0077】一方、読み出しワードが「(」でない場合(ステップS414、その他)には、さらにこの読み出したワードが「)」であるか否かを判断する(ステップS416)。この読み出したワードが「)」でない場合、すなわちその他である場合には、ステップS413に移行し、さらにACLから1ワードを読み出す。一方、この読み出したワードが「)」である場合には、NBが「0」であるか否かを判断する(ステップS417)。NBが「0」でない場合(ステップS417、NO)には、NBの値から「1」減算し、ステップS413に移行し、さらにACLから1ワード読み出す。

【0078】NBが「0」のとき(ステップS417、YES)には、ACLの現在位置の一つ手前を括弧内ACLの終点として記憶する(ステップS419)。その後、この括弧内ACLのライセンス生成処理を行い(ステップS420)、その再帰呼び出しによる戻り値をアクセス条件ACに追加する処理を行って(ステップS421)、ステップS400に移行する。これによって括弧内のACLが生成される。

【0079】一方、読み出したワードが「(」でない場合(ステップS410、その他)には、さらに、この読み出したワードが物理要素条件または会計条件であるか否かを判断する(ステップS410)。物理条件または会計条件である場合には、この条件をアクセス条件ACに設定し(ステップS431)、この条件を強制可能な物理要素の秘密キーKpとして設定し(ステップS432)、ステップS400に移行し、さらにACLから1ワード読み出す。

【0080】読み出したワードが物理条件または会計条件でない場合(ステップS410、その他)には、さらに、この読み出したワードが「OR」であるか否かを判断する(ステップS430)。読み出したワードが「OR」である場合には、この読み出したワードから後のACLのライセンス生成処理を行う(ステップS441)。その後、さらに生成したライセンスの中にACが含まれるか否かを判断し(ステップS442)、ACが含まれる場合(ステップS442、YES)には、ステップS441によるライセンス生成処理の戻り値を用いて「|AC, hash| Kp, 戻り値」となるライセンスに設定し(ステップS443)、この生成したライセンスを返す(ステップS454)。一方、ライセンスの中にACが含まれていない場合(ステップS442、NO)には、ステップS441によるライセンス生成処理の戻り値を用いて「|Kc, AC, hash| Kp, 戻り値」と

なるライセンスに設定し（ステップS445）、この生成したライセンスを返す（ステップS454）。

【0081】一方、読み出したワードが「OR」でない場合（ステップS430、その他）には、さらに、この読み出したワードが「AND」であるか否かを判断する（ステップS440）。読み出したワードが「AND」である場合には、この読み出したワードから後のACLのライセンス生成処理を行い（ステップS452）、このライセンス生成処理の戻り値を用いて「戻り値、AC、hash|Kp」となるライセンスを返す（ステップS454）。

【0082】さらに、この読み出したワードが「AND」でない場合（ステップS440、その他）には、「戻り値、AC、hash|Kp」となるライセンスを返す（ステップS454）。これにより、ACLからライセンスが生成される。

【0083】つぎに、図11に示すフローチャートを参照して、利用者システム50の内部処理手順について説明する。図11において、まず利用者システム50は、コンテンツの利用要求があったか否かを判断する（ステップS500）。コンテンツの利用要求がない場合（ステップS500、なし）には、この判断処理を繰り返し、コンテンツの利用要求があった場合（ステップS500、あり）には、コンテンツの利用要求を送信する（ステップS501）。その後、物理要素の証明書の要求がライセンスサーバ40からあったか否かを判断し（ステップS502）、物理要素の証明書の要求がない場合（ステップS502、なし）には、ステップS508に移行する。

【0084】一方、物理要素の証明書の要求があった場合（ステップS502、あり）には、物理要素ID証明書を読み出し（ステップS503）、読み出し失敗したか否かを判断する（ステップS504）。読み出しに失敗した場合（ステップS504、YES）には、エラー通知をライセンスサーバに送信して（ステップS505）、ステップS500に移行する。一方、読み出しに失敗しない場合（ステップS504、NO）には、つぎの物理要素があるか否かを判断し（ステップS506）、つぎの物理要素がある場合（ステップS506、あり）には、ステップS503に移行して、つぎの物理要素ID証明書の読み出しを行って上述した処理を繰り返す。

【0085】一方、つぎの物理要素がない場合（ステップS506、なし）には、物理要素ID証明書群をライセンスサーバ40に送信し（ステップS507）、さらに受信内容がエラーかライセンスかを判断する（ステップS508）。受信内容がエラーである場合（ステップS508、エラー）には、ステップS500に移行して上述した処理を繰り返し、受信内容がライセンスである場合（ステップS508、ライセンス）には、さらに、

ライセンスを物理要素（PCSUE）1に渡し（ステップS509）、ステップS500に移行して上述した処理を繰り返す。これにより、利用者システム50は、ライセンスサーバ40からライセンスを取得することができる。

【0086】ここで、PCSUE1とは、(N-1)個のPCSUEの最初のPCSUEを示し、一般的にPCSUE*i*で示し、*i*は、1～(N-1)の整数である。そこで、各PCSUE*i*がライセンスを渡された時の内部処理手順について図12のフローチャートを参照して説明する。

【0087】図12において、まずPCSUE*i*は、受信したライセンスをKp*i*で復号する（ステップ600）。その後、この復号したアクセス条件AC*i*を評価し（ステップS601）、アクセス条件AC*i*の評価結果が可か不可かを判断する（ステップS602）。アクセス条件AC*i*の評価結果が不可の場合（ステップS602、不可）には、エラー処理を行って（ステップS604）、本処理を終了する。一方、アクセス条件AC*i*の評価結果が可である場合（ステップS602、可）には、この復号したライセンスをPCSUE(*i*+1)に送信し、復号を続行させ、本PCSUE*i*の内部処理を終了する。

【0088】つぎに、PCSUE(*i*+1)は、PCSUE(N)に相当し、ここでは、たとえば、再生デバイスの物理要素が内部処理を行う。この内部処理手順について図13に示すフローチャートを参照して説明する。図13において、まず、受信したライセンスをKpnで復号する（ステップS700）。その後、この復号したアクセス条件AC(N)を評価し（ステップS701）、この評価結果が可であるか、不可であるかを判断する（ステップS702）。評価結果が不可である場合（ステップS702、不可）には、エラー処理を行って（ステップS703）、本処理を終了して、結果的に秘匿コンテンツを復号することができないことになる。

【0089】一方、アクセス条件AC(N)に対する評価結果が可である場合（ステップS702、可）には、この復号したKcで秘匿コンテンツを復号し（ステップS704）、復号したコンテンツを再生デバイスが再生し（ステップS705）、本処理を終了する。

【0090】ここで、具体的なライセンスの復号処理を図14を参照して説明する。図14において、ライセンスサーバ40で生成されたライセンスは、アクセス制御リストACLとコンテンツ復号キーとを再生デバイス144の物理要素IDであるキーKpを用いて暗号化し、さらに、ストレージデバイスのデバイスシリアル番号であるDSN141とメディア142のメディアシリアル番号であるMSN143の排他的論理和の値をキーとして暗号化されたものである。

【0091】まず、ストレージデバイス140は、メデ

イア 142 に書き込み不可の MSN を読み込み、この値とストレージデバイス 140 自身の DSN との排他的論理和の演算を行い、この演算結果によってライセンスを復号すると、ライセンスは、|ACL, Kc| Kp となる。この一部復号されたライセンスは、再生デバイス 144 に送られ、再生デバイス 144 は、再生デバイス 144 自身が有する物理要素 ID であるキー Kp を用いてライセンスを復号し、アクセス条件リスト ACL とコンテンツ復号キー Kc とを取得し、アクセス条件 ACL が示すアクセス条件を満足する場合に、コンテンツ復号キー Kc によって復号を行うことができ、復号されたコンテンツは、再生デバイス 144 によって再生されることになる。

【0092】 上述したライセンス要求とライセンス取得によるコンテンツ復号処理を図 15 に示すデータフローを参照してさらに説明する。図 15 において、利用者システム 50 内における復号保護領域では、まずコンテンツを利用するためライセンス要求処理 152 を物理要素 ID 証明書を送付してライセンスサーバ 40 に送出する。この際、物理要素 ID 証明書は、利用環境特定物理要素証明書取得処理 153 によって利用環境特定物理要素 150 から取得され、ライセンス要求処理 152 によって渡される。

【0093】 一方、ライセンスサーバ 40 からライセンスが送信されるとライセンス取得処理 156 は、このライセンスを取得し、アクセス許可処理 155 は、ライセンス所得処理 156 からライセンスを取得するとともに、利用環境特定物理要素 ID 認証処理 154 が利用環境特定物理要素証明書取得処理 153 を介して物理要素 ID を取得し、さらに会計処理 157 から利用状況を取得し、これらを用いて復号キーを取り出す。

【0094】 そして、コンテンツ復号処理 159 は、コンテンツ復号キーを用いて秘匿コンテンツ 158 を復号し、平文のコンテンツを出力する。なお、会計処理 157 は、利用状況監視物理要素 151 に通知し、利用環境監視物理要素 151 によって現在の利用状況が利用に応じて自動的にデクリメントされる。

【0095】 ところで、図 16 は、図 8 に示した特定利用環境の各エンティティに各処理手続きを実装した場合の保護強度への影響を示す図である。この結果から、利用環境特定物理要素所有証明書の生成は、デバイス層に実装し、会計情報保護は、IC カードによるデバイス層に実装することが好ましいことがわかる。このように、各処理手続きを実装するレイヤによっても保護強度が異なるので、レイヤ配置も考慮して図 15 に示す各処理機能を実装する必要がある。

【0096】 なお、上述した実施の形態では、いわゆるコンテンツキャッシュ可能型モデルを基準とした構成として説明したが、これに限らず、コンテンツ同時配布型モデルを基準とした構成にも適用できるのは明らかであ

る。この場合、コンテンツサーバ 30 がライセンスサーバ 40 内に内部配置された構成として取り扱えばよい。

【0097】 さらに、上述した実施の形態では、暗号化、復号化に関して、キーを用いることが前提となっているが、この場合において、秘密鍵暗号方式を用いても、公開鍵暗号方式を用いても、いずれでも実施可能であり、適応されるシステムに応じてそれぞれ適切な方式を適用すればよい。

【0098】 また、上述した実施の形態に示す物理要素には、利用者システム 50 に固定の装置のみではなく、この利用者システム 50 を利用する際に用いられるメディア、すなわち CD-ROM、DVD、MO、IC カードやフロッピーディスク等の可搬型の記録媒体を含むものである。この可搬型の記録媒体が用いられる利用者システムにおいては、この利用者システムに固定の物理要素に加えて、この用いられる可搬型の記録媒体も物理要素に含まれて、コンテンツの利用制御がなされることになる。なお、利用者システム 50 に固定のメディア、例えば固定のハードディスク装置や固定の ROM 等が上述した物理要素に含まれるのは言うまでもない。

【0099】

【発明の効果】 以上説明したように、本発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を記憶し、記憶した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成するよう構成したので、コンテンツの不正利用を精度高く防止することができるという効果を奏する。

【0100】 また、本発明によれば、復号鍵がコンテンツの復号に利用されるまでにライセンスが順に受け渡される物理要素の情報を登録し、登録した物理要素の情報に基づいて復号鍵および利用許可条件を暗号化してライセンスを生成するよう構成したので、コンテンツの不正利用を精度高く防止することができるという効果を奏する。

【図面の簡単な説明】

【図 1】 本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。

【図 2】 図 1 に示した著作権者システム 20 の内部処理手順を示すフローチャートである。

【図 3】 会計条件と物理環境特定要素条件との一例を示す図である。

【図 4】 図 1 に示したコンテンツサーバ 30 の内部処理手順を示すフローチャートである。

【図 5】 図 1 に示したライセンスサーバ 40 の内部処理手順を示すフローチャートである。

【図 6】 ライセンスサーバ 40 から送られるライセンスと著作権者システム 10 あるいはコンテンツサーバ 30 から送られる秘匿コンテンツとの関係を示す図である。

【図 7】 図 1 に示した LDAP システム 42 の構成を示

す図である。

【図 8】 特定利用環境のレイヤ論理構造を示す図である。

【図 9】 包含関係をもった物理要素の一例を示す図である。

【図 10】 ライセンス生成処理手順を示す詳細フローチャートである。

【図 11】 図 1 に示した利用者システム 50 の内部処理手順を示すフローチャートである。

【図 12】 利用関係特定物理要素によるライセンス復号処理手順を示すフローチャートである。

【図 13】 再生デバイスの物理要素によるライセンス復号処理手順を示すフローチャートである。

【図 14】 ライセンスの復号過程の一例を示す図である。

【図 15】 ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図である。

【図 16】 特定利用環境の各エンティティに各処理手続きを実装した場合における保護強度への影響を示す図である。

【図 17】 従来におけるアクセス制御モデルを示す図である。

【図 18】 従来におけるアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図である。

【図 19】 改良したアクセス制御モデルを示す図である。

【図 20】 従来におけるコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。

【図 21】 コンテンツキャッシュ可能型モデルを示す図

である。

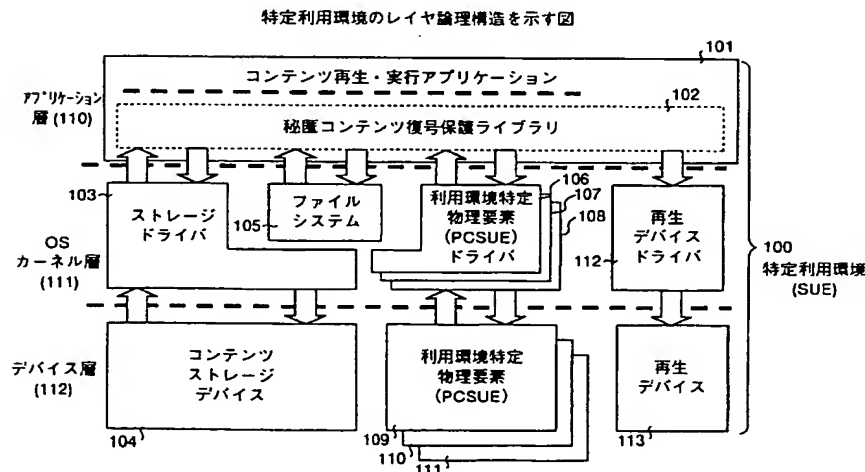
【図 22】 図 21 に示したコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示す図である。

【図 23】 コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図である。

【符号の説明】

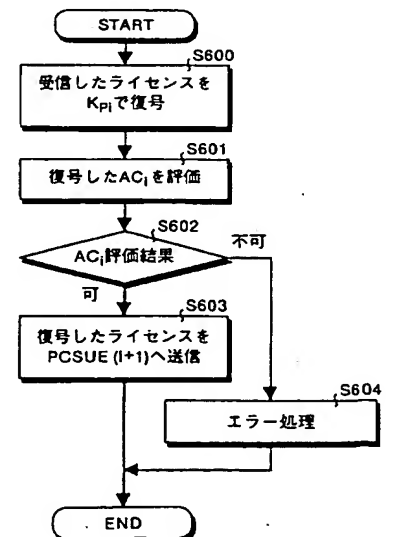
- | | |
|----------------|-----------------|
| 1 | 著作権者 |
| 2 | 利用者 |
| 10 | コンテンツ利用制御システム |
| 20 | 著作権者システム |
| 21 | 秘密コンテンツ登録部 |
| 22 | アクセス制御権委譲部 |
| 23 | ACL 設定部 |
| 30 | コンテンツサーバ |
| 40 | ライセンスサーバ |
| 41 | ライセンス許可／生成部 |
| 42 | LDAP システム |
| 43 | アクセス制御リスト (ACL) |
| 20 | 44 キー |
| 50 | 利用者システム |
| 51 | 秘匿コンテンツ要求／取得部 |
| 52 | ライセンス要求／取得部 |
| 53 | 特定利用環境 |
| 54-1 ~ 54-N | 利用環境特定物理要素 |
| 55-1 ~ 55-M | コンテンツストレージデバイス |
| 56-1 ~ 56-L | 再生デバイス |
| 57-1、59-1、61-1 | 物理要素 ID |
| 58-1、60-1、62-1 | 暗号化／復号化／評価 |
| 30 | 部 |

【図 8】

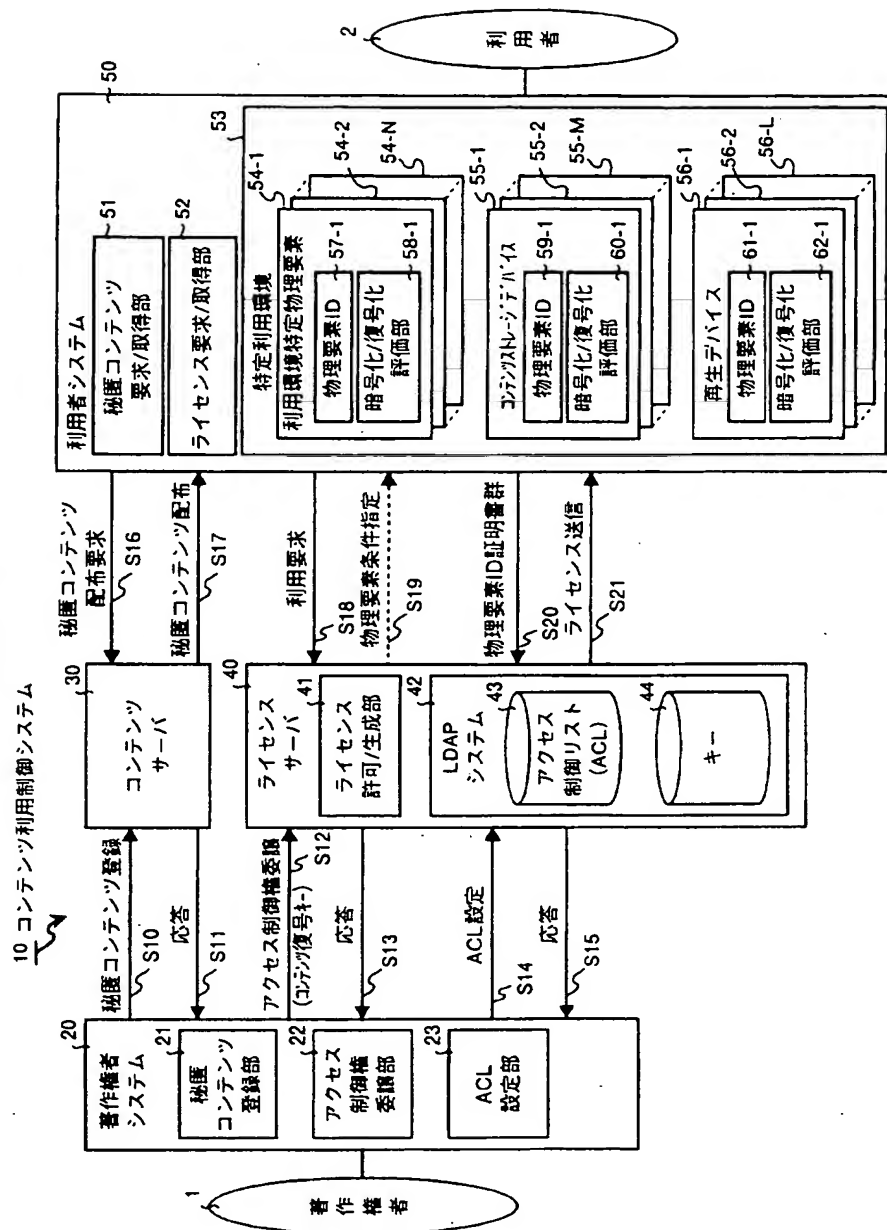


【図 12】

利用者関係特定物理要素によるライセンス復号処理手順を示すフローチャート

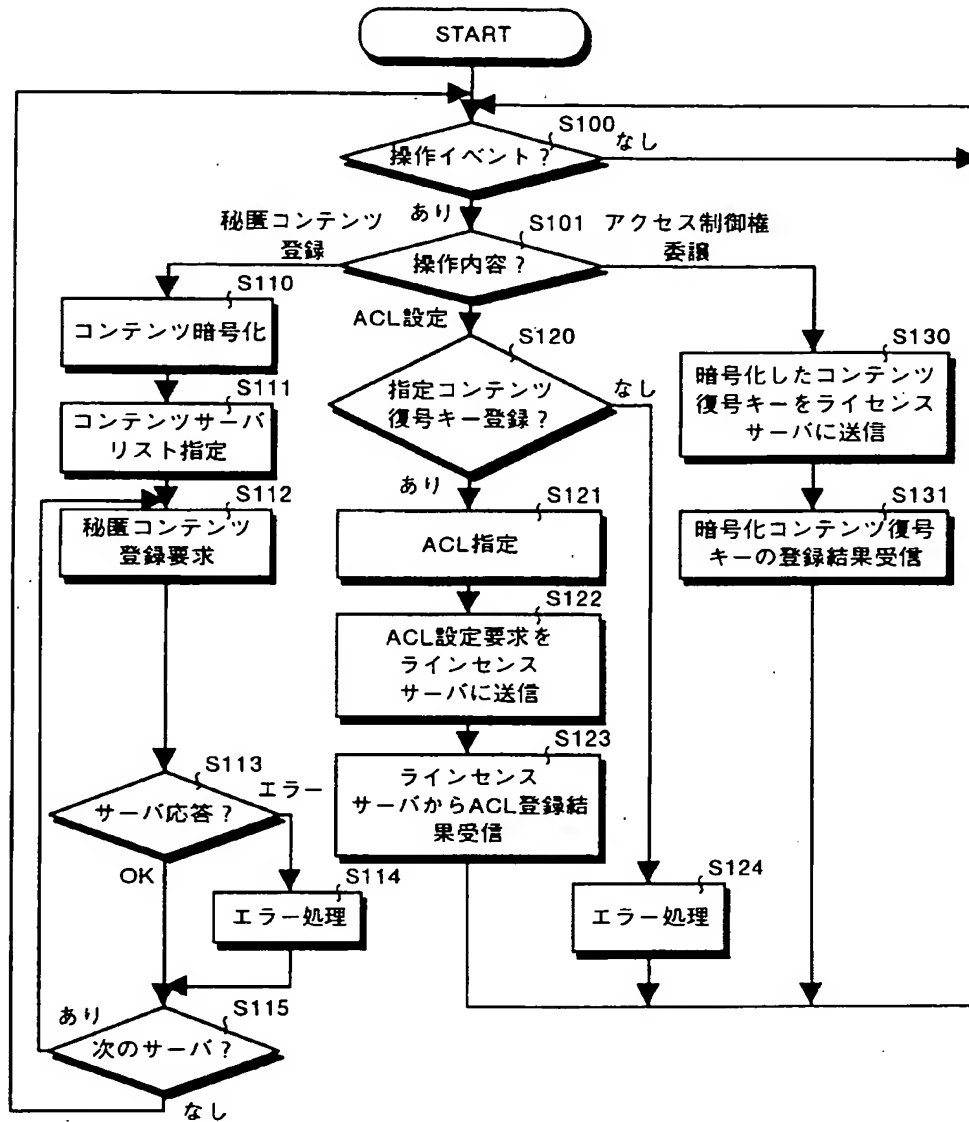


本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図



【図2】

図1に示した著作権システム20の内部処理手順を示すフローチャート



【図3】

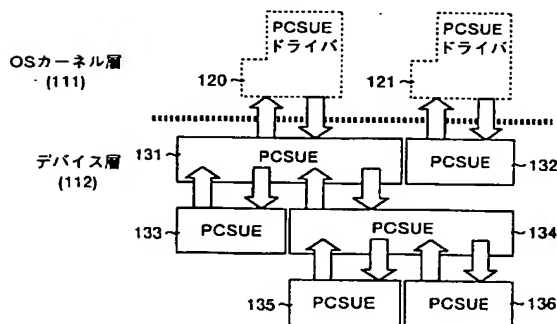
会計条件と物理環境特定要素条件との一例を示す図

会計条件値 (Account Condition Value)	利用状況 (Usage State)
max Count : 操作可能回数最大値	count : 操作済回数
max Length : 読み出し最大長さ	totalLen : 読み出し済長さ + 被要求読み出し長さ
max TimeLen : 実行可能最大時間	totalTime : 実行済時間長
max Debt : 借入可能金額 (課金条件)	debt : 残金 (マイナスは借入金額)

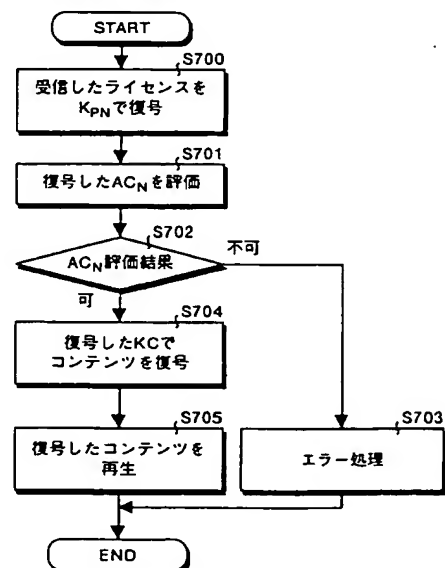
物理環境特定要素 (PCSUE) 条件	物理要素IDクラス (PCSUE-IDClass)
(1) 計算機本体	PSN (プロセッサシリアル番号)
(2) 周辺デバイス	DSN : デバイスの種別、シリアル番号
(3) メディア	MSN : メディアの種別、シリアル番号
(4) ICカード	certificates : ICカードが発行する証明書
(5) 人体部位 (指紋、網膜…)	body Parts : 人体部位 (指紋、網膜…) 認証情報
(6) 許可する時間帯	time Period : 時刻 (ローカルクロック、GPSなど)
(7) ネットワークドメイン	MACAddress : MACアドレス
(8) 地理的位置 (利用国など)	location : GPS/PHS検出位置
(9) 人の記憶	user-ID WithPwd : ユーザIDとパスワード
(10) グループ	group : 物理要素IDの集合

【図9】

包含関係をもった物理要素の一例を示す図

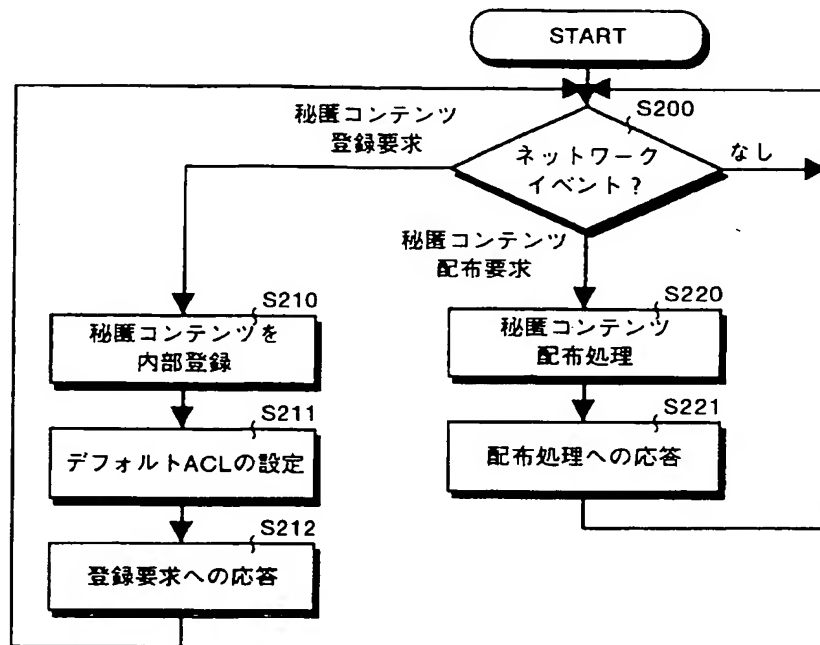


【図13】

再生デバイスの物理要素によるライセンス
復号処理手順を示すフローチャート

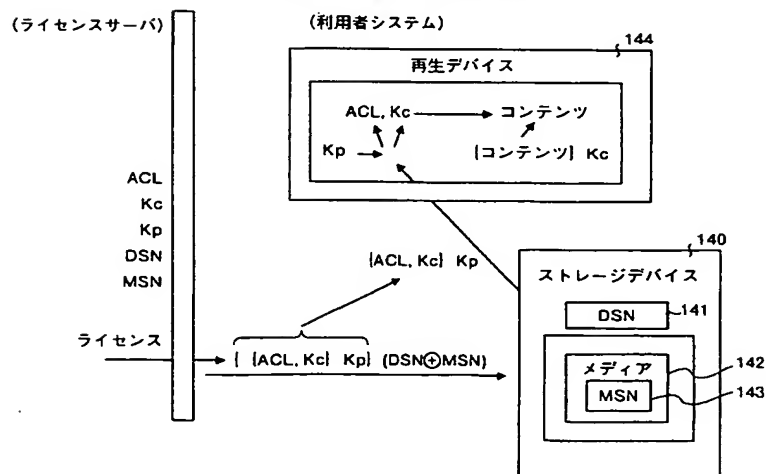
【図4】

図1に示したコンテンツサーバ30の内部処理手順を示すフローチャート



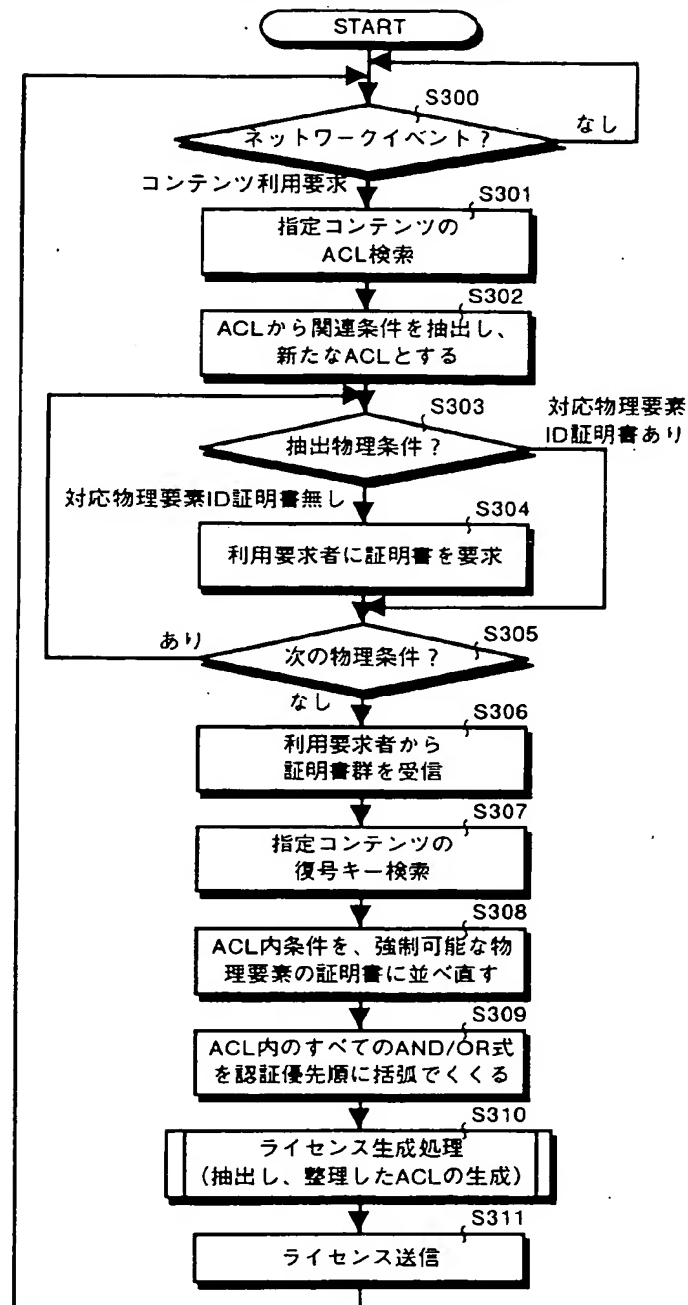
【図14】

ライセンスの復号課程の一例を示す図



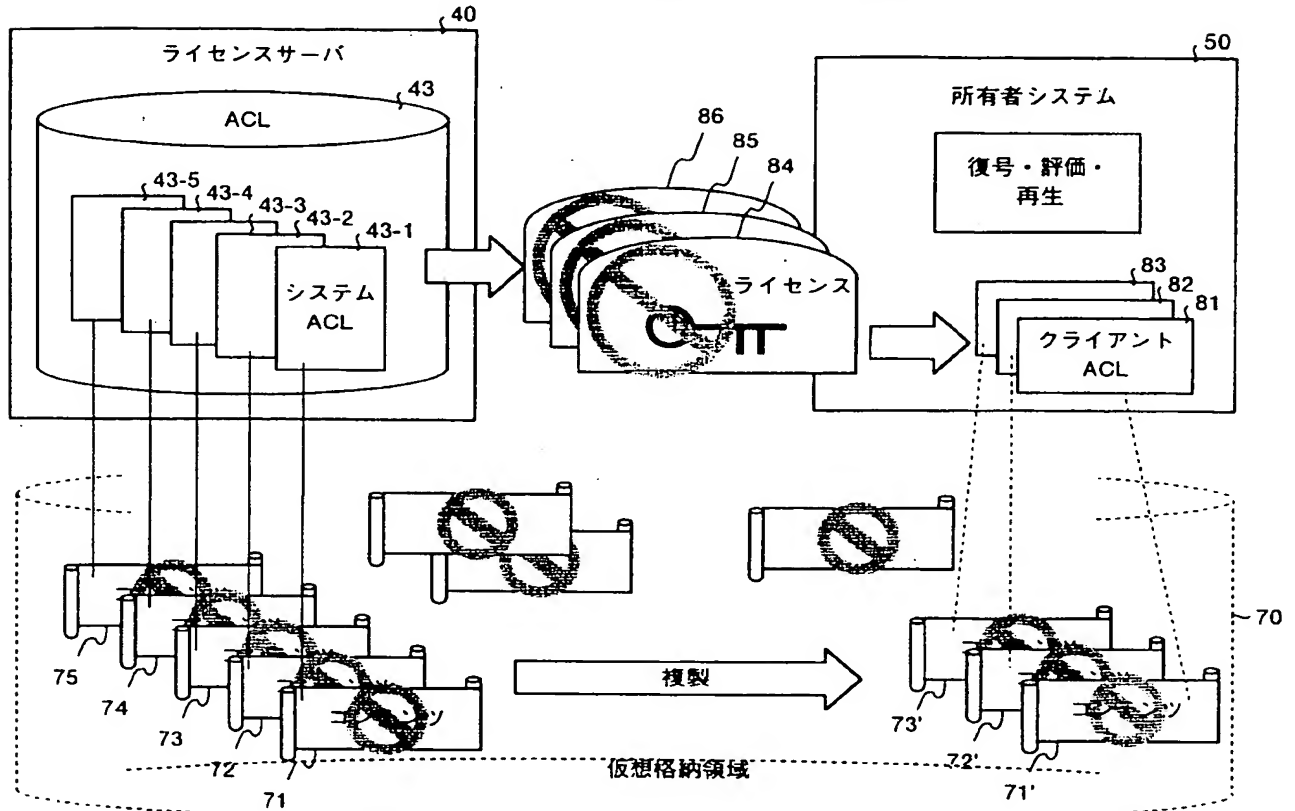
【図5】

図1に示したライセンスサーバ40の内部処理手順を示すフローチャート



【図6】

ライセンスサーバ40から送られるライセンスと著作権者システム10あるいは
コンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図



【図16】

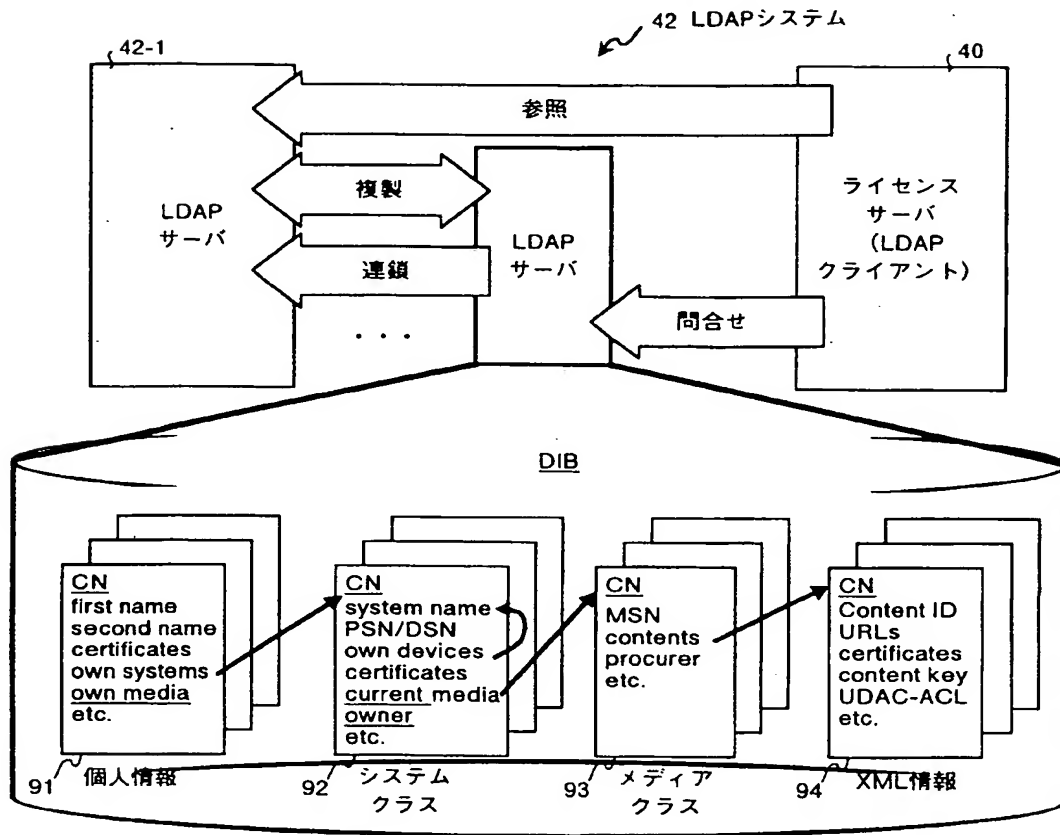
特定利用環境の各エンティティに各処理手続きを
実装した場合における保護強度への影響を示す図

	アプリケーション層	デバイスドライバ層	デバイス層
利用環境特定物理要素 所有証明書生成	—	○	●
利用環境特定物理要素 ID認証	○	—	—
アクセス制御リスト 検索	○	—	○
会計情報保護	△	—	● (ICカード)
条件付アクセス許可	○	—	○
復号	○	—	○

—：実装の意義が少ない △：危険 ○：専門家には保護が弱い ●：保護が強い

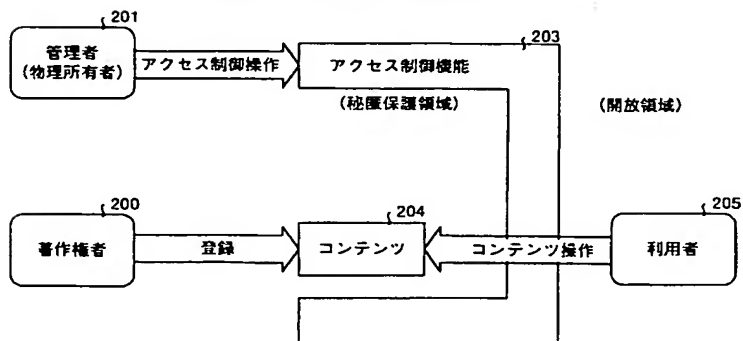
【図7】

図1に示したLDAPシステム42の構成を示す図



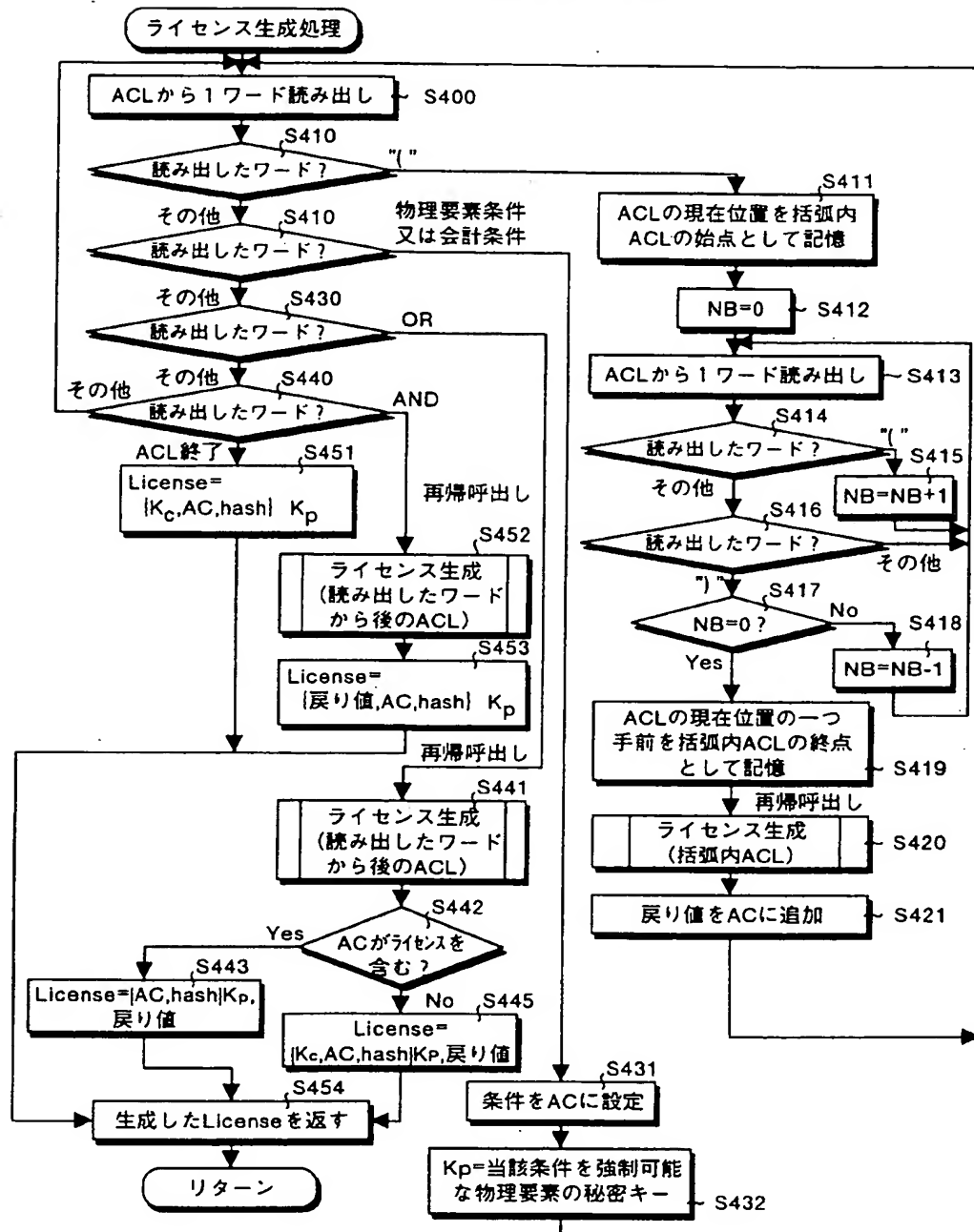
【図17】

従来のアクセス制御モデルを示す図



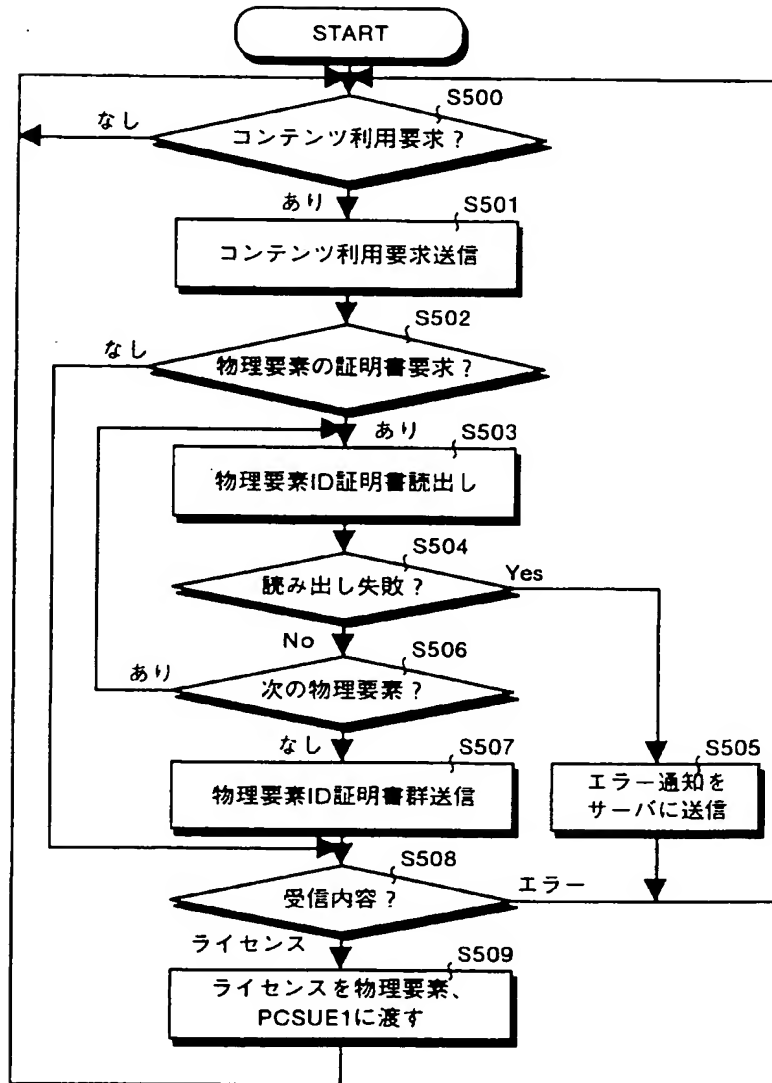
【図10】

ライセンス生成処理手順を示す詳細フローチャート



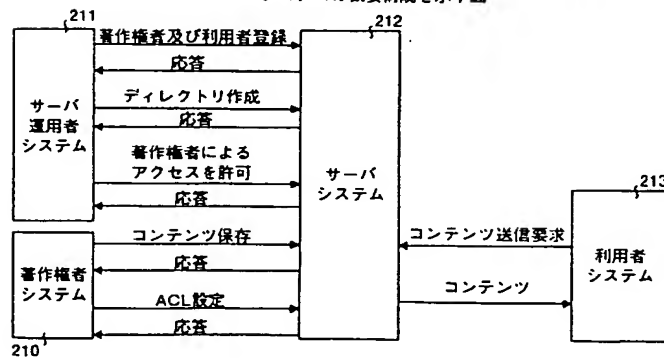
【図11】

図1に示した利用者システム50の内部処理手順を示すフローチャート

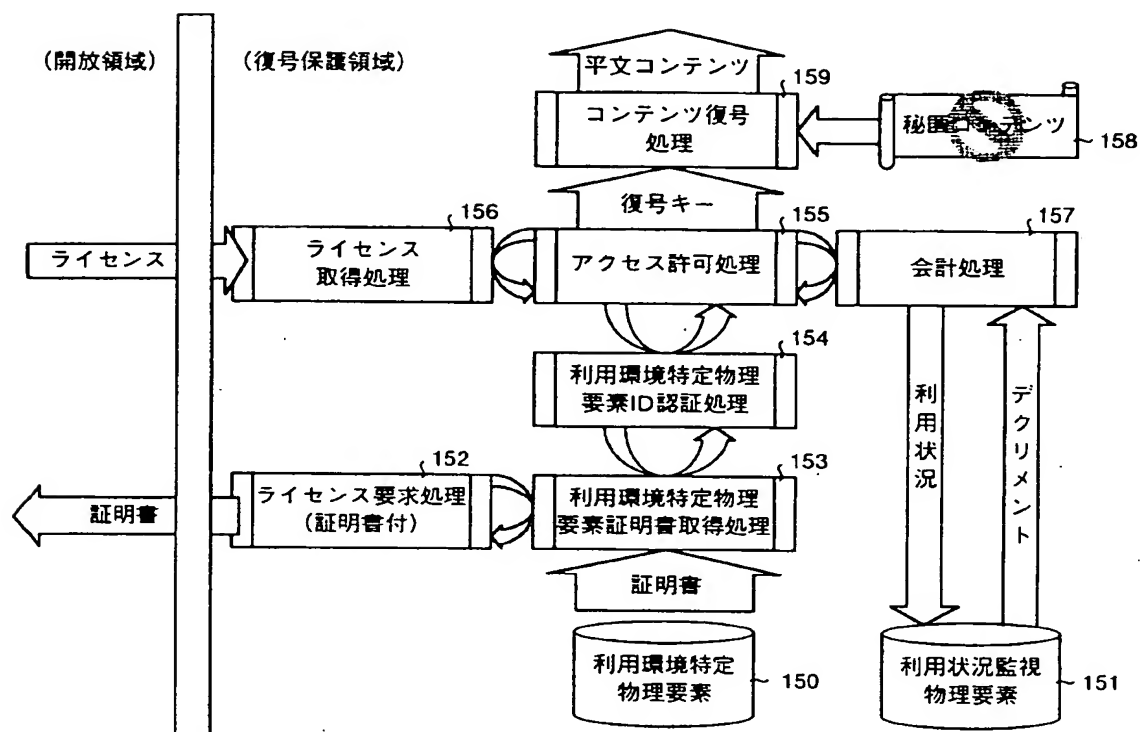


【図18】

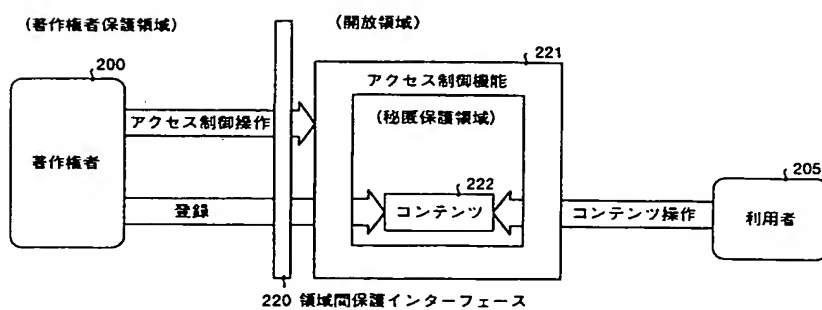
従来のアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図



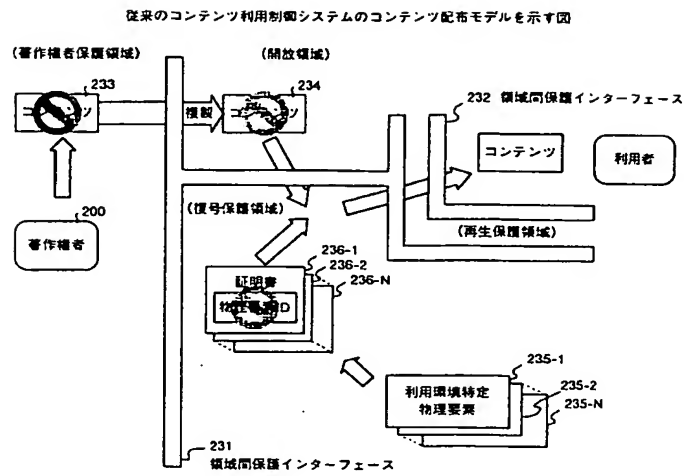
ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図



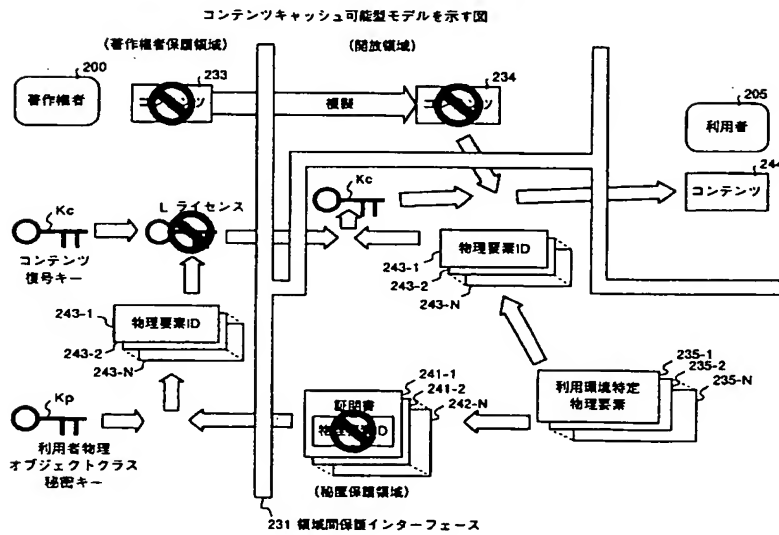
改良したアクセス制御モデルを示す図



【図20】

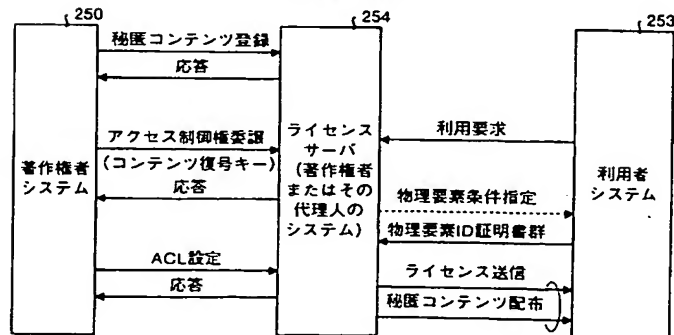


【図21】

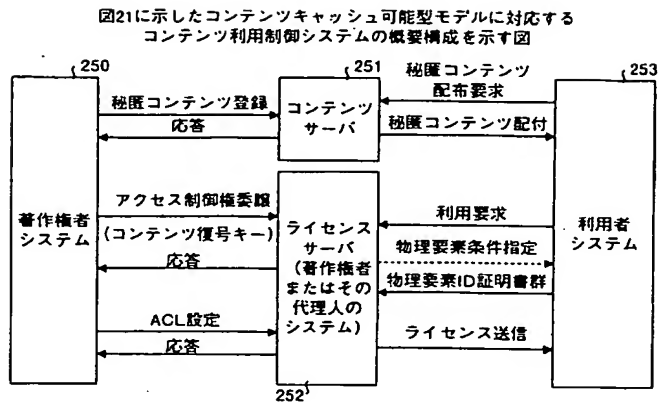


【図23】

コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図



【図22】



フロントページの続き

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-コ-ト*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D

(72)発明者 宮澤 雄司
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA03 AA06 BB09 BB10 CA16
5B085 AA08 AE08 AE23 AE29 BC02
BG02 BG07
5J104 AA12 AA16 EA04 EA15 MA01
NA02